Über die algebraischzahlentheoretische Verallgemeinerung eines elementarzahlentheoretischen Satzes von Zsigmondy.*)

Von LADISLAUS RÉDEI in Szeged.

Durchgängige Bezeichnungen und einige Benennungen:

„n" bezeichnet eine natürliche Zahl.

„ω" bezeichnet eine ganze algebraische Zahl.

„ω ist eine n-te Potenzzahl" soll bedeuten, daß ω die n-te Potenz eines Elementes des durch ω erzeugten Körpers ist. (Statt „n-te Potenzzahl" werde für $n=2, 3$ auch „Quadratzahl" bzw. „Kubikzahl" gesagt.)

„R" bezeichnet den Ring der ganzen rationalen Zahlen.

„R_ω" bezeichnet den Ring der ganzen Elemente des durch ω erzeugten Körpers. (Also $R_\omega = R$ für $\omega \in R$.)

„$\mathfrak{p}$" bezeichnet ein Primideal aus R_ω. (Üblicherweise werde stillschweigend $\mathfrak{p} \neq 0, R_\omega$ angenommen.) Diese Bezeichnung $\mathfrak{p}$ wird auch im Zusammenhang mit den unten zu definierenden $\omega_n, \omega_n^{(1)}, \ldots$ (statt ω) beibehalten.

„p" bezeichnet die durch $\mathfrak{p}$ teilbare Primzahl oder — wenn kein $\mathfrak{p}$ festgewählt wird — eine beliebige Primzahl.

„$N_\omega(\ldots), S_\omega(\ldots)$", kürzer „$N(\ldots), S(\ldots)$" bezeichnen die Norm eines Elementes oder Ideals bzw. die Spur eines Elementes von R_ω.

„$o(\ldots)$" bezeichnet die Ordnung $(=1, 2, \ldots, \infty)$ eines Elementes einer (multiplikativen) Gruppe (die stillschweigend auch Untergruppe irgendeiner vorgelegten algebraischen Struktur sein darf).

„$o(\omega(\mathrm{mod}\,\mathfrak{p}))$" bezeichnet für ein zu ω primes $\mathfrak{p}$ die Ordnung der Restklasse $\omega(\mathrm{mod}\,\mathfrak{p})$, anders die Ordnung von $\omega \bmod \mathfrak{p}$, d. h. das kleinste n mit $\omega^n \equiv 1 \,(\mathrm{mod}\,\mathfrak{p})$. (Man pflegt $o(\omega(\mathrm{mod}\,\mathfrak{p}))$ auch den Exponenten von $\omega \bmod \mathfrak{p}$ zu nennen.)

---

*) Erst nach der Fertigstellung des Manuskriptes dieser Arbeit wurde mir die Arbeit von H. Sachs, Untersuchungen über das Problem der eigentlichen Teiler, *Wiss. Zeitschrift d. Martin-Luther-Univ. Halle—Wittenberg*, **6**, Heft 2 (1956/57), 223—259 bekannt, in der ein allgemeineres Problem untersucht wird. Inhaltlich überschneiden sich beide Arbeiten nur sehr wenig.

„ω_n" bezeichnet ein ω mit unerfüllbarem $o(\omega \pmod{\mathfrak{p}}) = n$ und wird eine *exzeptionelle Zahl* (*für n*) genannt. Mehrere solche Zahlen werden auch mit $\omega_n^{(1)}, \omega_n^{(2)}, \ldots$ bezeichnet. Es ist klar, daß die Menge aller ω_n gegen Konjugiertenbildung invariant ist, weshalb konjugierte ω_n für gewöhnlich als nicht verschieden angesehen werden.

„a, b, c" bezeichnen Elemente von R.

„a_n, b_n" bezeichnen Elemente von R, deren sämtliche Primteiler in n aufgehen. Insbesondere bezeichnen also a_1, b_1 die Zahlen ± 1.

„Polynom" bedeutet hier stets ein Polynom über R.

„Hauptpolynom" bedeutet ein Polynom in einer Unbestimmten mit dem Anfangskoeffizienten 1.

„Grad..." bezeichnet den Grad einer algebraischen Zahl oder eines Primideals oder eines Polynoms.

„$f_\omega(x)$" bezeichnet das Minimalpolynom von ω, d. h. das irreduzible Hauptpolynom mit der Nullstelle ω. (Also ist Grad $f_\omega(x) = \text{Grad } \omega$.)

„ϱ" bezeichnet eine komplexe Zahl ($\neq 0$) mit $o(\varrho) = n$, d. h. eine primitive n-te komplexe Einheitswurzel.

„R_ϱ" bezeichnet also (als Spezialfall von R_ω) den Ring der ganzen Elemente des n-ten Kreisteilungskörpers.

„$F_n(x)$" bezeichnet das n-te Kreisteilungspolynom (ist also gleich $f_\varrho(x)$).

„$\varphi(n)$" ($= \text{Grad } \varrho = \text{Grad } F_n(x)$) bezeichnet die Eulersche Funktion.

„$\mu(n)$" bezeichnet die Möbiussche Funktion.

„$\mathfrak{p}^k \| \omega$" bezeichnet das Bestehen von $\mathfrak{p}^k | \omega$ und $\mathfrak{p}^{k+1} \nmid \omega$.

§ 1. Einleitung.

Wir beschäftigen uns mit den exzeptionellen Zahlen ω_n. Nach obiger Definition lassen sich diese auch so charakterisieren, daß $\omega_n^n - 1$ eine Einheit ist oder jeder Pimidealteiler von ihm schon in einem $\omega_n^d - 1$ ($d | n, < n$) aufgeht.

Die rationalen ω_n, d. h. die mit Grad $\omega_n = 1$, hat ZSIGMONDY [3] bestimmt. (Mit [ ] verweisen wir auf das Literaturverzeichnis am Schluß dieser Arbeit.) Sein diesbezüglicher interessanter Satz scheint sehr wenig bekannt zu sein und fand in der Literatur unseres Wissens bisher keine Anwendung. In einer anderen Arbeit [2] werden wir auf eine merkwürdige endlich-gruppentheoretische Folgerung dieses Satzes hinweisen. Hier untersuchen wir die ω_n bei beliebigem Grad ω_n und bekommen für sie weitgehende Aufklärungen, jedoch gelang uns ihre restlose Bestimmung nicht. Auf Grund unserer allgemeinen Resultate geben wir dann für den Satz von ZSIGMONDY einen neuen Beweis, der kürzer wird als der originale, ferner bestimmen wir die ω_n mit Grad $\omega_n = 2$ vollständig.

Satz 1. *Dann und nur dann ist* ω *ein* ω_n, *wenn* $F_n(\omega)$ *in einem* a_n *aufgeht.*

Korollar 1. *Sind* d, n *natürliche Zahlen und gehen alle Primteiler von* d *in* n *auf, so stimmen die* ω_{dn} *mit den* $\sqrt[d]{\omega_n}$ *überein.*

Da nämlich

$$F_{dn}(x) = F_n(x^d)$$

ist und die Zahlen a_{dn} mit den a_n übereinstimmen, so folgt Korollar 1 aus Satz 1.

Korollar 2. *Ist* n *ungerade, so stimmen die* ω_n *mit denjenigen* $-\omega_{2n}$ *überein, für die* $F_{2n}(\omega_{2n})$ *in einem* a_n *aufgeht.*

Da nämlich

$$F_{2n}(x) = F_n(-x)$$

ist, so folgt Korollar 2 aus Satz 1.

Man bemerke, daß das Problem der Bestimmung aller ω_n wegen Korollar 1 im wesentlichen auf den Fall von quadratfreien n zurückgeführt ist und man sich dabei wegen Korollar 2 auf die geraden n beschränken kann.

Korollar 3. *Eine komplexe Einheitswurzel* ω *ist dann und nur dann kein* ω_n, *wenn* $n \mid o(\omega)$ *gilt und* $\frac{o(\omega)}{n}$ $(\geqq 1)$ *die Potenz einer zu* n *primen Primzahl ist.*

Dem Beweis dieses Korollars schicken wir voraus, daß $\varrho - 1$ bekanntlich dann und nur dann keine Einheit ist, wenn $n = p^e$ $(e \geqq 0)$ ist, ferner gilt dann $(\varrho - 1, p) \neq 1$. Nunmehr berücksichtige man

$$F_n(\omega) = \prod_{\varrho} (\omega - \varrho),$$

wobei ϱ jetzt alle Einheitswurzeln mit $o(\varrho) = n$ durchläuft. Bis auf einen Einheitsfaktor stimmt die rechte Seite mit

$$\prod_{\varrho} (\omega \varrho^{-1} - 1)$$

überein. Nach voriger Bemerkung ist dieses Produkt offenbar dann und nur dann durch mindestens ein zu n primes Primideal teilbar, wenn die Bedingung von Korollar 3 erfüllt ist, weshalb dieses aus Satz 1 folgt.

Wegen

$$N_\omega(F_n(\omega))\,(= N_\omega(f_\varrho(\omega))) = (-1)^{\text{Grad}\,\omega\ \text{Grad}\,\varrho} N_\varrho(f_\omega(\varrho))$$

läßt sich Satz 1 auch so aussprechen:

Satz 1'. *Dann und nur dann ist ω ein ω_n, wenn $f_\omega(\varrho)$ in einem a_n aufgeht.*

Gleich zeigen wir, daß sich dieser Satz auch noch folgenderweise formulieren läßt:

Satz 1''. *Man nehme aus R_ϱ die in mindestens einem a_n aufgehenden Elemente, schreibe sie als $f(\varrho)$ mit Polynomen $f(x)$ vom Grad $< \varphi(n)$, lasse $g(x)$ alle Hauptpolynome durchlaufen und setze*

$$h(x) = g(x) F_n(x) + f(x).$$

Dann sind die (komplexen) Nullstellen der irreduziblen Polynome $h(x)$ und die der irreduziblen Hauptpolynome $f(x)$ eben die sämtlichen ω_n.

Die im Satz 1' genannte Bedingung läßt sich nämlich so aussprechen, daß das irreduzible Hauptpolynom $f_\omega(x)$ einem der im Satz 1'' genannten $f(x)$ mod $F_n(x)$ kongruent ist. Das beweist die Äquivalenz der Sätze 1', 1''.

Korollar 4. *Für jedes Paar n, k $(k = \varphi(n)+1, \varphi(n)+2, \ldots)$ gibt es unendlich viele ω_n mit Grad $\omega_n = k$.*

Denn nehme man ein $f(x)$ aus Satz 1''. Da $F_n(x)$ ein irreduzibles Hauptpolynom ist und $f(x) \neq 0$, Grad $f(x) <$ Grad $F_n(x)$ gelten, so ist

$$(x^l + z_1 x^{l-1} + \cdots + z_l) F_n(x) + f(x) \qquad (l = k - \varphi(n))$$

ein irreduzibles Element aus dem Polynomring $R[x, z_1, \ldots, z_l]$. Nach dem Irreduzibilitätssatz von HILBERT gewinnen wir also aus letzterem Polynom unendlich viele irreduzible Hauptpolynome k-ten Grades, indem wir $z_1, \ldots, z_l$ durch passende Elemente aus R ersetzen. Hieraus und aus Satz 1'' folgt somit Korollar 4.

Vermutung 1. Korollar 4 ist für $n > 1$, $k = \varphi(n)$ richtig.

Vermutung 2. Korollar 4 ist für $1 \leqq k < \varphi(n)$ falsch.

Über Vermutung 1 bemerken wir folgendes. Ist $p|n$, so wende man Satz 1'' mit $f(x) = p^t (t \geqq 0)$ und $g(x) = 1$ an. Es folgt, daß die Nullstellen derjenigen Polynome

$$F_n(x) + p^t,$$

die irreduzibel sind, lauter Zahlen ω_n mit Grad $\omega_n = \varphi(n)$ abgeben. In Hinsicht der Irreduzibilität darf man auf die Polynome

$$F_n(x+1) + p^t$$

übergehen. Da nun diese Polynome für $n = p^e (e \geqq 1)$, $t \geqq 2$ der Irreduzibilitätsbedingung von EISENSTEIN genügen, so folgt, daß Vermutung 1 für $n = p^e (> 1)$ richtig ist. Wir bemerken ferner, daß für $n = 2, 3, 4, 6$ nach den unten folgenden Sätzen 4, 5 beide Vermutungen richtig sind.

Eine wesentliche Verschärfung von Satz 1 liefert der folgende:

Satz 2. *Ist*

$$\mathfrak{p} \mid F_n(\omega_n), \tag{1}$$

weshalb nach Satz 1

$$n = p^e m,\ p^e \| n,\ e \geqq 1 \tag{2}$$

gesetzt werden kann, so gelten

$$m \mid p^{\text{Grad } \mathfrak{p}} - 1,\ o(\omega_n \pmod{\mathfrak{p}}) = m. \tag{3}$$

Besteht neben (1) *und* (2) *auch*

$$\mathfrak{p}^{\varphi(p^e)} \nmid p, \tag{4}$$

so geht $\mathfrak{p}$ *in* $F_n(\omega_n)$ *und* p *zu gleicher Potenz auf.*

Satz 3. *Die Anzahl der verschiedenen (rationalen) Primfaktoren von einem* $N(F_n(\omega_n))$ *ist je nach den Fällen Grad* $\omega_n \leqq 2$, *Grad* $\omega_n \geqq 3$ *höchstens gleich Grad* ω_n *bzw.* $-1 + \text{Grad } \omega_n$.

Satz 4. (ZSIGMONDY [3]). *Die sämtlichen rationalen* ω_n *sind*

$$\omega_1 = 2,\ \omega_2 = -1 + a_2,\ \omega_3 = -2,\ \omega_6 = 2,$$

außerdem noch $\omega_n = 0$ *für* $n = 1, 3, 4, 5, \ldots$, *ferner* $\omega_n = \pm 1$ *für* $n = 3, 4, 5, \ldots$.

Satz 5. *Die sämtlichen* ω_n *zweiten Grades sind*[1])[2])

$$\omega_1 = \frac{1}{2}(2 + a + \sqrt{a^2 + 4a_1}), \qquad S(\omega_1) = 2 + a, \qquad N(\omega_1) = 1 + a - a_1,$$

$$\omega_2 = \frac{1}{2}(-2 + a + \sqrt{a^2 + 4a_2}), \quad S(\omega_2) = -2 + a, \quad N(\omega_2) = 1 - a - a_2.$$

---

[1]) Die Fälle mit einer Quadratzahl unter dem Quadratwurzelzeichen sind außer Acht zu lassen; diese Ausnahmen sind (teils wegen Hilfssatz 11) offenbar die folgenden:

ω_1 für $a = \pm(1 - a_1)$;
ω_2 für $a = \pm(1 - a_2)$;
$\omega_3^{(1)}$ für $a_3 = -1, -3$; $\omega_3^{(2)}$ für $a_3 = 1, -3$; $\omega_3^{(3)}$ für $a_3 = -1, 3$; $\omega^{(4)}$ und $\omega^{(5)}$ für $a_3 = -1$; $\omega_3^{(6)}$ für $a_3 = \pm 1$
$\omega_4^{(1)}$ für $a_2 = 1, 2$; $\omega_4^{(2)}$ für $a_2 = \pm 2$; $\omega_4^{(3)}$ und $\omega_4^{(4)}$ für $a_2 = 1$;
$\omega_6^{(1)}$ für $a_6 = -1, -3$; $\omega_6^{(2)}$ für $a_6 = 1, -3$; $\omega_6^{(3)}$ für $a_6 = -1, 3$; $\omega_6^{(4)}$ und $\omega_6^{(5)}$ für $a_6 = -1$; $\omega_6^{(6)}$ für $a = \pm 1$.

[2]) Abgesehen von ganz einfachen Fällen haben wir im Satz 5 auch die Spur und Norm der exzeptionellen Zahlen $\omega_n, \omega_n^{(1)}, \ldots$ (d. h. im wesentlichen die Koeffizienten der definierenden Gleichungen dieser Zahlen) angegeben. Das wird den Beweis des Satzes bequemer machen. (Wir bemerken, daß man die exzeptionellen Zahlen von mindestens drittem Grade im allgemeinen gewiß durch ihre definierenden Gleichungen anzugeben zu bestreben hat.)

$$\begin{cases} \omega_3^{(1)} = \frac{1}{2}(-1+\sqrt{-3-4a_3}), & S(\omega_3^{(1)}) = -1, & N(\omega_3^{(1)}) = 1+a_3, \\ \omega_3^{(2)} = \frac{1}{2}(-1-a_3+\sqrt{-3+2a_3+a_3^2}), & S(\omega_3^{(2)}) = -1-a_3, & N(\omega_3^{(2)}) = 1, \\ \omega_3^{(3)} = \frac{1}{2}(-1-a_3+\sqrt{-3-2a_3+a_3^2}), & S(\omega_3^{(3)}) = -1-a_3, & N(\omega_3^{(3)}) = 1+a_3, \\ \omega_3^{(4)} = \frac{1}{2}(-1+a_3+\sqrt{(-3-6a_3+a_3^2}), & S(\omega_3^{(4)}) = -1+a_3, & N(\omega_3^{(4)}) = 1+a_3, \\ \omega_3^{(5)} = \frac{1}{2}(-1-a_3+\sqrt{(-3-6a_3+a_3^2}), & S(\omega_3^{(5)}) = -1-a_3, & N(\omega_3^{(5)}) = 1+2a_3, \\ \omega_3^{(6)} = \frac{1}{2}(-1-2a_3+\sqrt{(-3+4a_3^2}), & S(\omega_3^{(6)}) = -1-2a_3, & N(\omega_3^{(6)}) = 1+a_3, \end{cases}$$

$$\begin{cases} \omega_4^{(1)} = \sqrt{-1+a_2}, & & \\ \omega_4^{(2)} = \frac{1}{2}(a_2+\sqrt{-4+a_2^2}), & S(\omega_4^{(2)}) = a_2, & N(\omega_4^{(2)}) = 1 \\ \omega_4^{(3)} = \frac{1}{2}(a_2+\sqrt{-4+4a_2+a_2^2}), & S(\omega_4^{(3)}) = a_2, & N(\omega_4^{(3)}) = 1-a_2, \\ \omega_4^{(4)} = \frac{1}{2}(-a_2+\sqrt{-4+4a_2+a_2^2}), & S(\omega_4^{(4)}) = -a_2, & N(\omega_4^{(4)}) = 1-a_2, \end{cases}$$

$$\begin{cases} \omega_5^{(1)} = -1+\sqrt{-1}, \\ \omega_5^{(2)} = \frac{1}{2}(-3+\sqrt{5}), \end{cases}$$

$$\begin{cases} \omega_6^{(1)} = \frac{1}{2}(1+\sqrt{-3-4a_6}), & S(\omega_6^{(1)}) = 1, & N(\omega_6^{(1)}) = 1+a_6, \\ \omega_6^{(2)} = \frac{1}{2}(1+a_6+\sqrt{-3+2a_6+a_6^2}), & S(\omega_6^{(2)}) = 1+a_6, & N(\omega_6^{(2)}) = 1, \\ \omega_6^{(3)} = \frac{1}{2}(1+a_6+\sqrt{-3-2a_6+a_6^2}), & S(\omega_6^{(3)}) = 1+a_6, & N(\omega_6^{(3)}) = 1+a_6, \\ \omega_6^{(4)} = \frac{1}{2}(1-a_6+\sqrt{-3-6a_6+a_6^2}), & S(\omega_6^{(4)}) = 1-a_6, & N(\omega_6^{(4)}) = 1+a_6, \\ \omega_6^{(5)} = \frac{1}{2}(1+a_6+\sqrt{-3-6a_6+a_6^2}), & S(\omega_6^{(5)}) = 1+a_6, & N(\omega_6^{(5)}) = 1+2a_6, \\ \omega_6^{(6)} = \frac{1}{2}(1+2a_6+\sqrt{-3+4a_6^2}), & S(\omega_6^{(6)}) = 1+2a_6, & N(\omega_6^{(6)}) = 1+a_6, \end{cases}$$

$$\begin{cases} \omega_{10}^{(1)} = 1 + \sqrt{-1}, \\ \omega_{10}^{(2)} = \frac{1}{2}(3 + \sqrt{5}), \end{cases} \qquad \begin{cases} \omega_{12}^{(1)} = \sqrt{2}, \\ \omega_{12}^{(2)} = \frac{1}{2}(\pm 1 + \sqrt{5}), \\ \omega_{12}^{(3)} = \frac{1}{2}(\pm 3 + \sqrt{5}), \end{cases}$$

$$\omega_{20} = \frac{1}{2}(\pm 1 + \sqrt{5}), \qquad \omega_{24} = \frac{1}{2}(\pm 1 + \sqrt{5}),$$

außerdem noch die Einheitswurzeln $\sqrt{-1}$, $\frac{1}{2}(-1 + \sqrt{-3})$ *und* $\frac{1}{2}(1 + \sqrt{-3})$ *für* $n \neq 1, 4$ *bzw.* $n \neq 1, 3$, *bzw.* $n \neq 1, 2, 3, 6$.

§ 2. Beweis von Satz 1.

Um Satz 1 zu beweisen nehmen wir zuerst an, daß ω ein ω_n ist, und wollen zeigen, daß dann $F_n(\omega)$ Teiler eines a_n ist. Ist $F_n(\omega)$ eine Einheit, so ist das wahr. Im anderen Fall nehmen wir

$$\mathfrak{p} \mid F_n(\omega) \tag{5}$$

an. Noch mehr gilt dann

$$\mathfrak{p} \mid \omega^n - 1. \tag{6}$$

Wegen der Annahme folgt hieraus $o(\omega \pmod{\mathfrak{p}}) < n$, also die Existenz einer Primzahl q mit

$$q \mid n, \quad \mathfrak{p} \mid \omega^{\frac{n}{q}} - 1. \tag{7}$$

Da ferner

$$\frac{x^n - 1}{x^{\frac{n}{q}} - 1} \equiv q \pmod{x^{\frac{n}{q}} - 1} \tag{8}$$

besteht und die linke Seite durch $F_n(x)$ teilbar ist, so ergibt sich hieraus (bei der Ersetzung $x = \omega$) wegen (6) und (7_2) die Teilbarkeit $\mathfrak{p} \mid q$. Dies beweist wegen (7_1) die Behauptung, daß $F_n(\omega)$ in einem a_n aufgeht.

Umgekehrt, nehmen wir letzteres an. Wir haben zu zeigen, daß dann ω ein ω_n ist. Ist das falsch, so gibt es ein $\mathfrak{p}$ mit $o(\omega \pmod{\mathfrak{p}}) = n$. Dies bedeutet, daß (6) besteht und (7) für jede Primzahl q falsch ist. Wegen

$$\omega^n - 1 = \prod_{d \mid n} F_d(\omega), \qquad F_d(\omega) \mid \omega^d - 1$$

folgt hieraus die Erfülltheit von (5). Dies und die Annahme ergeben $\mathfrak{p} \mid n$, also

auch $p|n$. Hieraus, aus $p|N_\omega(\mathfrak{p})$ und aus dem Satz von FERMAT folgt

$$\omega^{\frac{n}{p}} \equiv \omega^{\frac{n}{p}N_\omega(\mathfrak{p})} \equiv 1 \pmod{\mathfrak{p}},$$

also $o(\omega(\mathrm{mod}\ \mathfrak{p})) < n$. Dies bedeutet, daß ω trotzdem ein ω_n ist. Mit diesem Widerspruch ist Satz 1 bewiesen.

§ 3. Beweis von Satz 2.

Hilfssatz 1. *Es sei $\alpha(\neq 1)$ ein Element von R_ω mit $\mathfrak{p}|\alpha-1$. Man setze*

$$\mathfrak{p}^k \| \alpha - 1, \qquad \mathfrak{p}^g \| p. \tag{9}$$

Gelten dann für eine natürliche Zahl e alle Ungleichheiten

$$\varphi(p^i)k \not\equiv g \qquad (i = 1, \ldots, e), \tag{10}$$

so gilt

$$\mathfrak{p}^{k_e} \| \alpha^{p^e} - 1 \tag{11}$$

mit

$$k_e = \min(p^e k, p^{e-1}k + g, p^{e-2}k + 2g, \ldots, k + eg). \tag{12}$$

Dem Beweis schicken wir voraus, daß offenbar

$$\min(pk_e, k_e + g) = k_{e+1} \tag{13}$$

und (wegen $\varphi(p)p^e = \varphi(p^{e+1})$)

$$\varphi(p)k_e = g \Longleftrightarrow \varphi(p^{e+1})k = g \tag{14}$$

gelten, wobei $\Longleftrightarrow$ für „dann und nur dann" steht.

Nunmehr beweisen wir Hilfssatz 1 zuerst für $e = 1$. Es gilt

$$\alpha^p - 1 = ((\alpha-1)+1)^p - 1 \equiv (\alpha-1)^p + p(\alpha-1) \pmod{p(\alpha-1)^2}. \tag{15}$$

Da ferner (10) für $e = 1$ als $(p-1)k \not\equiv g$, d. h. als $pk \not\equiv g + k$ lautet, so folgt aus (9) und (15)

$$\mathfrak{p}^{\min(pk,\, g+k)} \| \alpha^p - 1.$$

Der Exponent auf der linken Seite ist nach (12) gleich k_1, weshalb Hilfssatz 1 für $e = 1$ bewiesen ist.

Wir setzen dann Hilfssatz 1 für ein e voraus und beweisen ihn für $e+1$ wie folgt. Es sei (10) mit $e+1$ statt e erfüllt. Dies bedeutet das Erfülltsein von (10) selbst und wegen (14) das von $\varphi(p)k_e \not\equiv g$. Wegen des ersten und der Induktionsvoraussetzung besteht (11). Wegen des zweiten und der für $e = 1$ schon bewiesenen Richtigkeit von Hilfssatz 1 folgt also (mit Anwendung auf α^{p^e} statt α) das Bestehen von

$$\mathfrak{p}^{\min(pk_e,\, k_e+g)} \| \alpha^{p^{e+1}} - 1.$$

Wegen (13) ist hiermit Hilfssatz 1 allgemein bewiesen.

Hilfssatz 2. *Ist α ein Element von R_ω mit $\mathfrak{p}|\alpha-1$ und trifft*

$$\mathfrak{p}^{\varphi(p^e)} \nmid p \tag{16}$$

mit einem $e(\geqq 1)$ zu, so geht $\mathfrak{p}$ in

$$F_p(\alpha^{p^{e-1}}) \tag{17}$$

und p zu gleicher Potenz auf.

Im Fall $\alpha = 1$ ist (17) gleich p, weshalb jetzt die Behauptung trivial ist. Im übriggebliebenen Fall $\alpha \neq 1$ übernehmen wir die Bezeichnungen aus Hilfssatz 1. Wegen (9_2) läßt sich dann (16) als

$$\varphi(p^e) > g \tag{18}$$

schreiben.

Einerseits folgt hieraus

$$p^e k > p^{e-1}k + kg,$$

weshalb auf der rechten Seite von (12) sich das erste Glied streichen läßt, also

$$k_e = k_{e-1} + g \qquad (k_0 = k) \tag{19}$$

gilt.

Andererseits folgt aus (18) die Erfülltheit von (10), also nach Hilfssatz 1 die von (11) für alle $1, \ldots, e$ statt e. Letzteres und (9_1) besagen

$$\mathfrak{p}^{k_i} \| \alpha^{p^i} - 1 \qquad (i = 0, \ldots, e).$$

Man berücksichtige diese Relationen aber nur für $i = e, e-1$. Werden sie miteinander dividiert, so gewinnt man wegen (9_2) und (19) eben die Richtigkeit von Hilfssatz 2.

Nach diesen Vorbereitungen beweisen wir Satz 2. Um zuerst (3) zu beweisen setzen wir

$$m^* = o(\omega_n (\mathrm{mod}\ \mathfrak{p})), \text{ also } m^* | p^{\mathrm{Grad}\,\mathfrak{p}} - 1. \tag{20}$$

Dann braucht zur Bestätigung von (3) nur $m^* = m$ ausgewiesen zu werden.

Wegen (1) ist

$$\mathfrak{p} | \omega_n^n - 1. \tag{21}$$

Dies und (20_1) ergeben

$$m^* | n. \tag{22}$$

Andererseits bezeichne q einen von p verschiedenen Primteiler von n. Aus (1) und (8) folgt hierfür (bei der Ersetzung $x = \omega_n$)

$$\mathfrak{p} \nmid \omega_n^{\frac{n}{q}} - 1.$$

Hiernach und nach (20_1) ist

$$m^* \nmid \frac{n}{q}.$$

Dies besagt wegen (22), daß $\frac{n}{m^*}$ eine Potenz von p ist. Da ferner m^* wegen (20_2) zu p prim ist, so folgt wegen (2) die erhoffte Gleichheit $m^* = m$. Das beweist (3).

Um noch die andere Behauptung von Satz 2 zu beweisen setzen wir

$$\alpha = \omega_n^m. \tag{23}$$

Wendet man

$$\alpha \equiv \alpha^{N(\mathfrak{p})^k} (\mathrm{mod}\ \mathfrak{p})$$

mit genügend großem k an, so folgt aus (2), (21), (23) das Bestehen von $\mathfrak{p} | \alpha - 1$. Hieraus, aus (4) und (23) folgt nach Hilfssatz 2, daß $\mathfrak{p}$ in

$$F_n(\omega_n^{p^{r-1}m}) \tag{24}$$

und p zu gleicher Potenz aufgeht.

Nun entsteht aber aus

$$F_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}$$

nach Abtrennung der zu $d = 1, p$ gehörenden Faktoren die Gleichung

$$F_n(x) = F_p(x^{\frac{n}{p}}) \prod_d{}' (x^{\frac{n}{d}} - 1)^{\mu(d)}, \tag{25}$$

wobei d die von 1, p verschiedenen quadratfreien Teiler von n durchzulaufen hat. Für diese ist $\frac{n}{d}$ wegen (2) kein Vielfaches von m, also ist für sie wegen der schon bewiesenen Beziehung (3_2)

$$\mathfrak{p} \nmid \omega_n^{\frac{n}{d}} - 1.$$

Wird also in (25) $x = \omega_n$ eingesetzt und (2) berücksichtigt, so besagt das über (24) Festgestellte eben die Richtigkeit der noch zu beweisenden Behauptung von Satz 2.

§ 4. Beweis von Satz 3.

Satz 3 ist richtig, wenn $F_n(\omega_n)$ eine Einheit ist. Im anderen Falle seien

$$p < p_2 < \cdots < p_k \qquad (k \geqq 1) \tag{26}$$

die verschiedenen Primteiler von $N(F_n(\omega_n))$, die also nach Satz 1 in n aufgehen.

Da insbesondere $(p, F_n(\omega_n)) \neq 1$ ist, so trifft (1) mit einem Primidealteiler $\mathfrak{p}$ von p zu, weshalb sich (2) wieder ansetzen läßt. Also besteht dann

$$p_2 \dots p_k | m.$$

Andererseits wenden wir aus Satz 2 jetzt nur (3_1) an. Hieraus und aus Vorigem folgt

$$p_2 \dots p_k | p^{\text{Grad}\,\mathfrak{p}} - 1.$$

Rechts darf wegen (26) durch $p-1$ dividiert werden. Wird dann „|" durch „$\leqq$" ersetzt, so hat man wieder wegen (26) und wegen $\text{Grad}\,\mathfrak{p} \leqq \text{Grad}\,\omega_n$

$$(1+p)^{k-1} \leqq 1 + p + p^2 + \dots + p^{-1+\text{Grad}\,\omega_n}.$$

Je nach den drei Fällen

$$\text{Grad}\,\omega_n = 1, = 2, \geqq 3$$

folgt hieraus der Reihe nach

$$k-1 = 0, \leqq 1, < -1 + \text{Grad}\,\omega_n,$$

d. h.

$$k = 1, \leqq 2, \leqq -1 + \text{Grad}\,\omega_n.$$

Da aber k eben die Anzahl der verschiedenen Primteiler von $N(F_n(\omega_n))$ bedeutet, so ist hiermit Satz 3 bewiesen.

§ 5. Beweis von Satz 4.

Hilfssatz 3. *Ist $n = p^e m$ mit $p^e \| n$, $e \geqq 1$ und α eine komplexe Zahl mit $|\alpha| > 1$, so gilt*

$$|F_n(\alpha)| \geqq \left(\frac{|\alpha|^{p^e} - 1}{|\alpha|^{p^{e-1}} + 1} \right)^{\varphi(m)}.$$

Da nämlich

$$F_n(\alpha) = F_m(\alpha^{p^e}) F_m(\alpha^{p^{e-1}})^{-1}, \qquad F_m(x) = \prod_{\sigma} (x - \sigma) \tag{27}$$

bestehen, wobei σ die $\varphi(m)$ komplexen Einheitswurzeln mit $o(\sigma) = m$ durchläuft, so folgt wegen $|\sigma| = 1$ die Richtigkeit von Hilfssatz 3.

Um Satz 4 zu beweisen betrachten wir ein ω_n mit

$$\text{Grad}\,\omega_n = 1. \tag{28}$$

Wir haben zu zeigen, daß diese ω_n eben die im Satz 4 aufgezählten sind.

Insbesondere lassen sich die ω_1 und ω_2 nach Satz 1 durch

$$(F_1(\omega_1) =)\, \omega_1 - 1 = a_1 \text{ bzw. } F_2(\omega_2) =)\, \omega_2 + 1 = a_2$$

charakterisieren. Diese bedeuten $\omega_1 = 1 + a_1 (= 1 \pm 1 = 2, 0)$ bzw. $\omega_2 = -1 + a_2$. Hiernach ist Satz 4 für $n = 1, 2$ richtig.

Trivial ist 0 für alle n ein ω_n, weshalb Satz 4 für $\omega_n = 0$ richtig ist. Ferner ist $\omega_n = 1$ bzw. $\omega_n = -1$ nach Korollar 3 genau für $n = 2, 3, 4, \ldots$ bzw. für $n = 1, 3, 4, \ldots$ erfüllt, also ist Satz 4 auch für $\omega_n = \pm 1$ richtig.

Wegen des Bewiesenen dürfen wir uns fortan auf den Fall

$$n \geqq 3, \quad |\omega_n| \geqq 2 \tag{29}$$

beschränken.

Wegen (28) lautet jetzt (3_1) als $m \mid p-1$. Hiernach folgt aus Satz 2, daß in $F_n(\omega_n)$ keine andere Primzahl als der größte Primteiler von n aufgehen kann. Fortan werde dieser mit p bezeichnet und

$$n = p^e m, \quad p^e \| n, \quad e \geqq 1 \tag{30}$$

gesetzt, wobei wegen (29_1)

$$p^e \geqq 3 \tag{31}$$

gilt. Da hiernach $\varphi(p^e) \geqq 2$, also (4) erfüllt ist, so folgt aus Satz 2 sogar

$$F_n(\omega_n) \mid p. \tag{32}$$

Andererseits sind wegen (29_2) und (30) die Voraussetzungen von Hilfssatz 3 mit $\alpha = \omega_n$ erfüllt. Aus diesem folgt wegen (29_2) und (31) noch mehr

$$|F_n(\omega_n)| > \left(\frac{1}{2}\,|\omega_n|^{\varphi(p^e)}\right)^{\varphi(m)} \geqq |\omega_n|^{(\varphi(p^e)-1)\varphi(m)} \tag{33}$$

Da stets $2^{p-1} \geqq p$ ist, so folgt aus (29_2), (32), (33)

$$(\varphi(p^e)-1)\varphi(m) \leqq p-2.$$

Dies ergibt wegen (31), daß im Fall der Existenz eines ω_n mit (28) und (29) notwendig

$$e = 1, \quad p \geqq 3, \quad \varphi(m) = 1 \tag{34}$$

gelten muß. Ferner folgt hieraus und aus (32), (33)

$$|\omega_n|^{p-2} < p. \tag{35}$$

Wegen (29_2) muß also $p \leqq 3$, somit wegen (34_2) $p = 3$ sein. Dies und $(34_{1,3})$ besagen, daß nur noch $n = 3, 6$ in Frage kommen, ferner folgt aus (29_2), (35) und $p = 3$, daß dabei notwendig $|\omega_n| = 2$, d.h. $\omega_n = \pm 2$ gelten muß.

Für die so übriggebliebenen insgesamt vier Möglichkeiten gelten (wegen $F_3(x) = x^2 + x + 1$, $F_6(x) = x^2 - x + 1$)

$$F_3(2) = 7, \quad F_3(-2) = 3, \quad F_6(2) = 3, \quad F_6(-2) = 7.$$

Satz 1 berücksichtigend sind wir also zum Schluß gekommen, daß die Bedingungen (28), (29) genau nur mit $\omega_3 = -2$, $\omega_6 = 2$ erfüllt sind. Dies mit den vor (29) erhaltenen Resultaten zusammen beweist Satz 4.

Der Leser sieht, daß in diesem Beweis aus Satz 1 im wesentlichen nur der Teil „nur dann“ und aus Korollar 3 nur ein trivialer Teil benutzt wurde, ferner sich der benutzte Teil von Satz 2 sich viel kürzer als selbst dieser Satz beweisen ließe.

§ 6. Erster Teil des Beweises von Satz 5.

Zum Beweis von Satz 5 haben wir die sämtlichen ω_n mit

$$\text{Grad } \omega_n = 2 \tag{36}$$

zu ermitteln. Der größeren Übersichtlichkeit halber spalten wir den Beweis in drei Teile auf, indem wir hier die quadratfreien geraden n, im § 7 die quadratfreien ungeraden n, im § 8 die übrigen n an die Reihe nehmen. Vorangehend erledigen wir aber gleich hier den Fall $|\omega_n| = 1$ und zwar für alle n.

Im Fall $|\omega_n| = 1$ ist ω_n wegen (36) nicht reell, also eine Einheitswurzel, und zwar kommen wieder wegen (36) nur

$$o(\omega_n) = 3, 4, 6$$

in Betracht. In diesen drei Fällen sind nach Korollar 3 die sämtlichen ungeeigneten n der Reihe nach die folgenden:

$$n = 1, 3 \quad \text{bzw.} \quad n = 1, 4 \quad \text{bzw.} \quad n = 2, 3, 6.$$

Die geeigneten n sind also zunächst in allen drei Fällen die $n = 5, 7, 8, 9, \ldots$, ferner noch einzeln in diesen drei Fällen der Reihe nach

$$n = 2, 4, 6 \quad \text{bzw.} \quad n = 2, 3, 6 \quad \text{bzw.} \quad n = 1, 4.$$

Das beweist Satz 5 für $|\omega_n| = 1$ und berechtigt uns fortan die Annahme

$$|\omega_n| \neq 1 \tag{37}$$

zu machen.[3])

Hilfssatz 4. *Ist $p \| n$, $n = pm$ und α eine komplexe Zahl mit $|\alpha| > 1$, so gilt*

$$|F_n(\alpha)| \geqq ((|\alpha| - 1)|\alpha|^{p-2})^{\varphi(m)}.$$

Da nämlich

$$|\alpha|^p - 1 \geqq |\alpha|^p - |\alpha|^{p-2} = (|\alpha| - 1)(|\alpha| + 1)|\alpha|^{p-2}$$

ist, so folgt Hilfssatz 4 aus Hilfssatz 3.

---

[3]) Einen Teil der gewünschten ω_n werden wir (wie auch in Satz 5) mit Formeln angeben, in denen a_2, a_3 oder a_6 als Variablen auftreten. Für einige ganz wenige Werte dieser Variablen wird dabei Grad $\omega_n = 1$ oder $|\omega_n| = 1$ ausfallen. Diese ω_n (für die also (36) oder (37) nicht zutrifft) werden stillschweigend außer Acht zu lassen, was hier ein für allemal bemerkt wurde.

Hilfssatz 5. *Ist* $p \| n, p \neq 2, n = pm$ *und* α *eine reelle Zahl mit* $|\alpha| < 1$, *so gilt*

$$|F_n(\alpha)| > \left(\frac{1}{2}\right)^{\varphi(m)}.$$

Dem Beweis schicken wir voran, daß für zwei reelle Zahlen u, v und eine komplexe Zahl σ mit

$$0 < u < v < 1, \quad |\sigma| = 1$$

stets

$$\left|\frac{u-\sigma}{v-\sigma}\right| > \frac{1}{2} \tag{38}$$

ist.

Bezeichnet nämlich σ' die zu σ konjugiert komplexe Zahl, so ist (38) gleichbedeutend mit

$$4(u^2-(\sigma+\sigma')u+1) > v^2-(\sigma+\sigma')v+1.$$

Es genügt dies für die beiden Extremalwerte $\sigma+\sigma' = \pm 2$ zu zeigen. Dabei handelt es sich um

$$4(u-1)^2 > (v-1)^2 \quad \text{und} \quad 4(u+1)^2 > (v+1)^2.$$

Das zweite ist trivial. Das erste ist gleichbedeutend mit $2(1-u) > 1-v$, d. h. mit $1+v > 2u$. Da dies zutrifft, so ist (38) bewiesen.

Aus (27) (angewendet mit $e = 1$) und aus (38) (angewendet mit $u = \alpha^p, v = \alpha$) folgt Hilfssatz 5 für positive α sofort. Da ferner (38) mit $-u, -v$ statt u, v richtig bleibt, so ist der Fall eines negativen α dem vorigen ähnlich.

Wir schicken noch voran, daß nach Satz 1 sich die ω_n als die ganzen algebraischen Zahlen mit

$$N(F_n(\omega_n)) = b_n \tag{39}$$

charakterisieren lassen. Da ferner für ein ω mit Grad $\omega = 2$ die Formel

$$\omega = \frac{1}{2}(S(\omega) + \sqrt{S(\omega)^2 - 4N(\omega)}) \tag{40}$$

gilt, so folgt, daß sich die ω_n mit Grad $\omega_n = 2$ auch durch

$$F_n(\omega_n) = \frac{1}{2}(a + \sqrt{a^2 + 4a_n}) \tag{41}$$

charakterisieren lassen. (Dabei wurde (39) mit $-a_n$ statt b_n angewendet, was ja gestattet ist, da beide dieselben Zahlen durchlaufen.)

Nach diesen Vorbereitungen wollen wir in diesem Paragraphen, wie gesagt, weiter nur die quadratfreien geraden n betrachten, und unterscheiden die Fälle $n = 2, n = 6, n > 6$.

Im Fall $n=2$ bekommen wir aus (41) wegen $F_2(x)=x+1$ die sämtlichen Lösungen unseres Problems in der Form

$$\omega_2=\frac{1}{2}(-2+a+\sqrt{a^2+4a_2}) \quad (\text{mit } N(F_2(\omega_2))=-a_2). \tag{42}$$

(Mit der hierbei in Klammern gesetzten Bemerkung haben wir spätere Zwecke.) Wegen (42) ist Satz 5 für $n=2$ richtig.

Im Fall $n=6$ nehmen wir die definierende Gleichung eines ω_6 bequemlichkeitshalber in der Form

$$\omega_6^2-(1+b)\omega_6+1+c=0 \tag{43}$$

an. Dann ist

$$F_6(\omega_6)=\omega_6^2-\omega_6+1=b\omega_6-c,$$

also (wieder wegen (43))

$$N(F_6(\omega_6))=b^2(1+c)-bc(1+b)+c^2=b^2-bc+c^2. \tag{44}$$

Somit besagt die Bedingung (39) für die ω_6 das Bestehen von

$$b^2-bc+c^2=b_6. \tag{45}$$

(Offenbar kommt dabei nur ein positives b_6 in Frage.)

Wir behaupten, daß die sämtlichen Lösungen b, c dieser Gleichung durch die Tabelle

(46)

b	0	a_6	a_6	$-a_6$	a_6	$2a_6$
c	a_6	0	a_6	a_6	$2a_6$	a_6
$N(F_6(\omega_6))$	a_6^2	a_6^2	a_6^2	$3a_6^2$	$3a_6^2$	$3a_6^2$

angegeben sind (wobei wir nach (44) jedesmal auch $N(F_6(\omega_6))$ berechnet haben).

Da nämlich die linke Seite von (45) homogen ist, so genügt es einzusehen, daß die der Bedingung $(b,c)=1$ unterworfenen zwölf („primitiven") Lösungen von (45) eben durch (46) mit $a_6=\pm 1$ geliefert sind. Das ist aber klar, da dann b_6 (>0) quadratfrei und ungerade, also nur 1 oder 3 sein kann, weshalb es sich jetzt um die b, c mit

$$b^2-bc+c^2=1 \quad \text{oder } 3$$

handelt. Somit ist die Behauptung über (46) bewiesen.

Nach (43) ist

$$\omega_6=\frac{1}{2}(1+b+\sqrt{(1+b)^2-4(1+c)}).$$

Werden hier b, c aus (46) eingesetzt, so entstehen eben die in Satz 5 aufgezählten $\omega_6^{(1)}, \ldots, \omega_6^{(6)}$. Somit ist dieser Satz für $n=6$ richtig.

Im Fall $n > 6$ bezeichnen wir mit p den maximalen Primteiler von n und setzen

$$n = pm, \tag{47}$$

wobei also (da n quadratfrei ist)

$$p \geqq 5,\ p \nmid m \tag{48}$$

gelten.

Dann zeigen wir vor allem, daß sich jetzt die ω_n als die ganzen algebraischen Zahlen mit

$$N(F_n(\omega_n)) \mid p^2 \tag{49}$$

charakterisieren lassen.

Wir haben nur zu zeigen, daß jetzt aus (39) das Bestehen von (49) folgt. Es genügt ein ω_n zu betrachten, wofür $N(F_n(\omega_n))$ keine Einheit ist. Wir bezeichnen mit p_0 einen Primteiler von dieser Norm. Wegen (39) muß $p_0 \mid n$ gelten, weshalb wir mit einer natürlichen Zahl m_0

$$n = p_0 m_0$$

setzen können, ferner hat p_0 nach der Annahme einen Primidealteiler $\mathfrak{p}_0$ mit

$$\mathfrak{p}_0 \mid F_n(\omega_n).$$

Wegen Grad $\mathfrak{p}_0 \leqq 2$ folgt aus Satz 2 zunächst

$$m_0 \mid p_0^2 - 1, \quad \text{d. h.} \quad m_0 \mid (p_0 - 1)(p_0 + 1).$$

Hieraus und aus (48_1) folgt (da p der maximale Primteiler von n ist), daß p kein Teiler von m_0 sein kann, d. h. notwendig

$$p_0 = p$$

ist. Indem wir entsprechend $\mathfrak{p}_0 = \mathfrak{p}$ setzen, so ist (4) (wieder wegen (48_1)) erfüllt, weshalb aus Satz 2 weiter folgt, daß $\mathfrak{p}$ in $F_n(\omega_n)$ und p zu gleicher Potenz aufgeht. Das hat (49) zur Folgerung, beweist somit die Behauptung.

Nunmehr wollen wir vor allem die nichtreellen ω_n bestimmen. Dann muß nach (49)

$$|F_n(\omega_n)| \leqq p$$

sein. Hieraus, aus (37), (47) und Hilfssatz 3 folgt

$$\left(\frac{|\omega_n|^p - 1}{|\omega_n| + 1}\right)^{\varphi(m)} \leqq p. \tag{50}$$

Hiernach und nach (48_1) muß noch mehr

$$\frac{|\omega_n|^5 - 1}{|\omega_n| + 1} \leqq 5$$

bestehen, weshalb $|\omega_n| < \sqrt{3}$[4]), d. h. $N(\omega_n) < 3$ ist. Dies und (37) ergeben

$$N(\omega_n) = 2, \quad \text{d. h.} \quad |\omega_n| = \sqrt{2}. \tag{51}$$

Da

$$\frac{(\sqrt{2})^{10} - 1}{\sqrt{2} + 1} > \frac{31}{3} > 10$$

ist, so folgt aus (50), (51) $p < 10$, also (wegen (48_1))

$$p = 5 \quad \text{oder} \quad p = 7.$$

Entsprechend lautet (50) wegen (51) als

$$(9 - 5\sqrt{2})^{\varphi(m)} \leqq 5 \quad \text{bzw.} \quad (17 - 9\sqrt{2})^{\varphi(m)} \leqq 7,$$

woraus $\varphi(m) < 4$ bzw. $\varphi(m) < 2$ folgt. Da aber m quadratfrei und gerade ist, so sind nur $m = 2, 6$ bzw. $m = 2$ möglich. Nach (47) kommen also nur

$$n = 10, 30, 14 \tag{52}$$

in Frage.

Andererseits läßt (51) nur die Fälle

$$\omega_n = \pm 1 + \sqrt{-1}, \quad \frac{1}{2}(\pm 1 + \sqrt{-7}) \tag{53}$$

zu. Unter den durch (52), (53) zugelassenen insgesamt 12 Möglichkeiten trifft aber (49) nach leichter Rechnung nur für den einzigen Fall $n = 10$, $\omega_{10} = 1 + \sqrt{-1}$ zu. Dies bedeutet, daß für ein quadratfreies gerades $n\,(> 6)$ nur ein einziges nichtreelles ω_n, nämlich

$$\omega_{10} = 1 + \sqrt{-1} \qquad (\text{mit } N(F_{10}(\omega_{10})) = 5) \tag{54}$$

existiert.

Wir haben noch die (49) befriedigenden reellen ω_n (für ein quadratfreies gerades $n > 6$) zu bestimmen. Man nehme ein solches ω_n an und bezeichne mit ω_n' sein Konjugiertes. Dabei darf

$$|\omega_n| \geqq |\omega_n'| \tag{55}$$

angenommen werden, woraus freilich

$$|\omega_n| > 1 \tag{56}$$

folgt. Wir unterscheiden zwei Fälle, je nachdem $|\omega_n'|$ kleiner oder größer als 1 ist.

Im Fall

$$|\omega_n'| < 1 \tag{57}$$

[4]) Wie hier so auch später fassen wir oft eine reelle Quadratwurzel stillschweigend als eine positive Zahl auf. Der Leser wird leicht sehen, wann das nötig ist.

gilt nach (47), (48), (49), (56) und den Hilfssätzen 3,5

$$\left(\frac{|\omega_n|^p-1}{2(|\omega_n|+1)}\right)^{\varphi(m)} < p^2. \tag{58}$$

Wegen (48$_1$) folgt hieraus

$$\frac{|\omega_n|^5-1}{2(|\omega_n|+1)} < 25,$$

also

$$|\omega_n| < 3. \tag{59}$$

Dies und (57) ergeben $|N(\omega_n)| < 3$, d. h. $|N(\omega_n)| = 1$ oder 2. Hieraus und aus (56), (59) folgt, daß nur

$$|\omega_n| = \frac{1}{2}(1+\sqrt{5}), \quad 1+\sqrt{2}, \quad 1+\sqrt{3}, \quad \frac{1}{2}(3+\sqrt{5})$$

in Frage kommen. Diese vier Fälle betrachten wir der Reihe nach.

Für

$$|\omega_n| = \frac{1}{2}(1+\sqrt{5}) \quad \text{(d. h.} \quad \omega_n = \pm\frac{1}{2}(1+\sqrt{5})\text{)}$$

hat man

$$\frac{|\omega_n|^{16}-1}{2(|\omega_n|+1)} > 16^2,$$

woraus wegen (58) $p < 16$, also wegen (48$_1$)

$$p = 5, 7, 11, 13$$

folgt. Wieder wegen (58) muß im ersten Fall $\varphi(m) < 5$ sein; da jetzt $5 \nmid m$, $2 | m$ ist, so hat man $m = 2$ oder 6. Im zweiten Fall folgt ähnlich $\varphi(m) < 4$, also wieder $m = 2$ oder 6. Im dritten und vierten Fall bekommt man $\varphi(m) < 2$, also $m = 2$. Somit kommen nach (47) nur

$$n = 10, 30, 14, 42, 22, 26$$

in Frage, jedoch trifft (49) nach leichter Rechnung in keinem dieser insgesamt 12 Fälle zu.

Für

$$|\omega_n| = 1+\sqrt{2} \quad \text{(d. h.} \quad \omega_n = \pm(1+\sqrt{2})\text{)}$$

hat man

$$\frac{|\omega_n|^7-1}{2(|\omega_n|+1)} > 7^2,$$

woraus wegen (58) $p < 7$, also $p = 5$ folgt, ferner ergibt sich aus (58) $\varphi(m) < 2$, $m = 2$, $n = 10$. Jedoch ist dabei (49) nicht erfüllt.

Für

$$|\omega_n| = 1+\sqrt{3} \qquad \text{(d. h.} \quad \omega_n = \pm(1+\sqrt{3})\text{)}$$

hat man

$$\frac{|\omega_n|^5-1}{2(|\omega_n|+1)} > 5^2,$$

weshalb jetzt sogar schon (58) mit keinem m erfüllt ist.

Für

$$\omega_n = \frac{1}{2}(3+\sqrt{5}) \qquad (\text{d. h. } \omega_n = \pm\frac{1}{2}(3+\sqrt{5}))$$

hat man

$$\frac{|\omega_n|^7-1}{2(|\omega_n|+1)} > 7^2,$$

woraus wegen (58) $p<7$, also $p=5$, und weiter hieraus $\varphi(m)<2$, $m=2$, $n=10$ folgt. Da

$$N\left(F_{10}\left(\frac{1}{2}(3+\sqrt{5})\right)\right)=5^2, \quad N\left(F_{10}\left(-\frac{1}{2}(3+\sqrt{5})\right)\right)=11^2$$

gelten, so ist (49) im ersten Fall erfüllt, im zweiten nicht erfüllt.

Wir haben bekommen, daß für ein quadratfreies gerades $n\,(>6)$ nur ein einziges, der Bedingung (57) unterworfenes reelles ω_n, nämlich

$$\omega_{10} = \frac{1}{2}(3+\sqrt{5}) \qquad (\text{mit } N(F_{10}(\omega_{10}))=5^2) \tag{60}$$

existiert.

Zu betrachten ist noch der Fall

$$|\omega_n'|>1. \tag{61}$$

Hieraus und aus (47), (49), (55) folgt nach Hilfssatz 3

$$\left(\frac{|\omega_n|^p-1}{|\omega_n|+1}\,\frac{|\omega_n'|^p-1}{|\omega_n'|+1}\right)^{\varphi(m)} \leqq p^2. \tag{62}$$

Genau so folgt nach Hilfssatz 4

$$((|\omega_n|-1)(|\omega_n'|-1)|\omega_n\omega_n'|^{p-2})^{\varphi(m)} \leqq p^2. \tag{63}$$

Wegen (55), (61) ist

$$|N(\omega_n)| = |\omega_n\omega_n'| \geqq 2.$$

Hiernach läßt sich

$$|\omega_n| = \frac{1}{2}(a+\sqrt{a^2\pm 4b}) \qquad (a\geqq 0,\ b\geqq 2) \tag{64}$$

ansetzen. Die beiden Fälle „$\pm$“ untersuchen wir getrennt.

Zuerst sei

$$|\omega_n| = \frac{1}{2}(a+\sqrt{a^2+4b}) \qquad \left(\text{also } |\omega_n'| = \frac{1}{2}(-a+\sqrt{a^2+4b})\right). \tag{65}$$

Dann folgt aus (61)

$$-a+\sqrt{a^2+4b}>2,\quad a^2+4b>(a+2)^2,\quad b>a+1,$$

also

$$a\leqq b-2. \tag{66}$$

Ferner lautet (63) wegen (65) als

$$((b+1-\sqrt{a^2+4b})b^{p-2})^{\varphi(m)}\leqq p^2. \tag{67}$$

(Freilich dürfte „=“ wegen der Irrationalität der linken Seite gestrichen werden.)

Wäre $b\geqq 4$, so folgte aus (48_1) und (67)

$$(b+1-\sqrt{a^2+4b})\,4^3<5^2.$$

Hiernach ist der erste Faktor kleiner als $\frac{1}{2}$, also folgt (teils aus (66))

$$\left(b+\frac{1}{2}\right)^2<a^2+4b\leqq b^2+4.$$

Dies ergibt $b+\frac{1}{4}<4$, $b<4$. Wegen dieses Widerspruchs muß $b\leqq 3$ sein.

Wenn $b=3$ ist, so folgt aus (66) $a\leqq 1$. Wegen (67) muß also

$$((4-\sqrt{13})3^{p-2})^{\varphi(m)}\leqq p^2$$

bestehen. Dies ergibt $p<7$, (wegen (48_1)) $p=5$, ferner $\varphi(m)<2$, $m=2$, somit (wegen (47)) $n=10$. Nach (65) kommen also jetzt für ω_n nur

$$\omega_{10}=\sqrt{3},\ \pm\frac{1}{2}(1+\sqrt{13})$$

in Frage. Jedoch ist (49) in diesen Fällen nicht erfüllt.

Im restlichen Fall $b=2$ muß wegen (66) $a=0$ sein. Hiernach und nach (65) ist

$$\omega_n=\pm\sqrt{2}.$$

Hierfür bekommt man aus (62)

$$\left(\frac{(\sqrt{2})^p-1}{\sqrt{2}+1}\right)^{\varphi(m)}\leqq p.$$

Dies ergibt zunächst $p<10$, also $p=5$ oder $p=7$. Ferner folgt für diese Fälle $\varphi(m)<3$, also $m=2, 6$ bzw. $\varphi(m)<2$, also $m=2$. Wegen (47) kommen somit nur $n=10, 30, 14$ in Frage. Jedoch ist dabei (49) nicht erfüllt. Somit haben wir die Möglichkeit (65) widerlegt.

Es bleibt noch aus (64) die andere Möglichkeit

$$|\omega_n|=\frac{1}{2}(a+\sqrt{a^2-4b}) \qquad (\text{also } |\omega_n'|=\frac{1}{2}(a-\sqrt{a^2-4b}) \tag{68}$$

zu untersuchen übrig. Wegen (61) muß dann

$$a-\sqrt{a^2-4b}>2,\ (a-2)^2>a^2-4b,\ -a+1>-b,$$

also

$$a \leqq b \tag{69}$$

sein. Ferner nimmt (63) wegen (68) die Form

$$((b+1-a)b^{p-2})^{\tau(m)} \leqq p^2.$$

an. Hieraus und aus (69) folgt

$$b^{p-2} \leqq p^2,$$

also (wegen (48_1)) $b<3$. Da aber $b \geqq 2$ ist, so folgt $b=2$. Dies mit (69) und $a \geqq 0$ zusammen widerspricht nach (68) der Reellität von ω_n.

Dies und die bei (54), (60) ausgesprochenen Resultate besagen, daß Satz 5 für die quadratfreien geraden $n(>6)$ richtig ist. Vereinigt mit den vorher erledigten Fällen $n=2, 6$ bedeutet das die Richtigkeit dieses Satzes für alle quadratfreien geraden n.

§ 7. Zweiter Teil des Beweises von Satz 5.

Auf Grund der eben erledigten Fälle beweisen wir jetzt Satz 5 für die quadratfreien ungeraden n mit Hilfe von Korollar 2. Nach diesem werden nämlich die ω_n für die gesagten n in der Form

$$\omega_n = -\omega_{2n} \tag{70}$$

erhalten, wobei rechts genau nur die ω_{2n} mit $N(F_{2n}(\omega_{2n}))=a_n$ und Grad $\omega_{2n}=2$ einzusetzen sind. Dabei kommen also nur die n mit $2n=2, 6, 10$, d. h. die $n=1, 3, 5$ in Frage.

Nun liefert diese Regel (70) angewendet mit $n=1, 3, 5$ (unter Berücksichtigung der bei (42), (46), (54), (60) hingestellten Normen) den Beweis von Satz 5 für diese n.

§ 8. Dritter Teil des Beweises von Satz 5.

Hilfssatz 6. *Ein ω mit Grad $\omega=2$ ist dann und nur dann eine Quadratzahl, wenn das Gleichungssystem*

$$y^2=N(\omega),\quad x^2=2y+S(\omega) \qquad (x, y \in R) \tag{71}$$

lösbar ist. Ist das der Fall, so liefern die Lösungen die sämtlichen Werte von $\sqrt{\omega}$ in der Form

$$\sqrt{\omega}=\frac{1}{2}(x+\sqrt{x^2-4y}). \tag{72}$$

Hilfssatz 7. *Ein ω mit Grad $\omega = 2$ ist dann und nur dann eine Kubikzahl, wenn das Gleichungssystem*

$$y^3 = N(\omega), \quad x^3 - 3xy = S(\omega) \qquad (x, y \in R) \tag{73}$$

lösbar ist. Ist das der Fall, so liefern die Lösungen die sämtlichen Werte von $\sqrt[3]{\omega}$ in der Form

$$\sqrt[3]{\omega} = \frac{1}{2}(x + \sqrt{x^2 - 4y}). \tag{74}$$

Diese zwei Hilfssätze sind Spezialfälle eines allgemeinen Satzes von uns [1]. Übrigens wird hier der zweite Teil von Hilfssatz 7 nicht benutzt.

Hilfssatz 8. *Es ist $1 + a_6$ genau nur für*

$$a_6 = -1, 3, 8, 24, 48, 288$$

eine Quadratzahl.

Denn es gibt unter den negativen a_6 offenbar nur die einzige Lösung $a_6 = -1$. Nachher sei $a_6 > 0$. Als Potenzen von 2 oder 3 sind bekanntlich genau nur $a_6 = 8$ bzw. $a_6 = 3$ passend. Nachher sei $6 | a_6$. Damit $1 + a_6$ eine Quadratzahl ist, muß dann sogar $8 | a_6$, also $24 | a_6$ sein. Wir setzen

$$1 + a_6 = 1 + 2^i 3^j = (1 + 6a)^2 \qquad (i \geqq 3, j \geqq 1)$$

an. Es folgt

$$2^{i-2} 3^{j-1} = a(1 + 3a).$$

Da unter den zwei Faktoren rechts der eine gerade, der andere ungerade ist, so muß im Fall $j = 1$ gewiß $a = \pm 1$ sein. Die entsprechenden Lösungen sind $a_6 = 7^2 - 1 = 48$ und $a_6 = (-5)^2 - 1 = 24$. Im Fall $j > 1$ muß

$$a = 3^{j-1} b, \quad 3 \nmid b, \quad 2^{i-2} = b(1 + 3^j b)$$

sein. Hieraus folgt $b = \pm 1$, also

$$\text{entweder } b = 1, \ 2^{i-2} = 1 + 3^j \quad \text{oder} \quad b = -1, \ 2^{i-2} = -1 + 3^j.$$

Da $j \geqq 2$ ist, so folgt im ersten Fall $i \geqq 5$, $8 | 1 + 3^j$, was offenbar unmöglich ist. Im zweiten Fall folgt ähnlich

$$i \geqq 4, \ 4 | -1 + 3^j, \ 2 | j; \ 2^{i-1} = (3^{\frac{j}{2}} + 1)(3^{\frac{j}{2}} - 1), \ 3^{\frac{j}{2}} - 1 = 2, \ j = 2, \ a = -3,$$

weshalb nur noch die Lösung $a_6 = (1 - 6 \cdot 3)^2 - 1 = 17^2 - 1 = 288$ entsteht. Das beweist Hilfssatz 8.

Hilfssatz 9. *Es ist $-1 + a_6$ genau nur für*

$$a_6 = 1, 2$$

eine Quadratzahl.

Denn aus $-1 + a_6 = a^2$ folgt sofort $3 \nmid a_6$, $4 \nmid a_6$, also $a_6 | 2$, ferner folgt $a_6 > 0$, weshalb nur $a_6 = 1, 2$ übrigbleiben.

Hilfssatz 10. *Es ist* $3+a_6$ *genau nur für*

$$a_6 = -3, -2, 1, 6$$

eine Quadratzahl.

Denn aus $3+a_6=a^2$ folgt sofort $4 \nmid a_6$, $9 \nmid a_6$, also $a_6 | 6$, ferner folgt $a_6 \geqq -3$. Hieraus entsteht die Behauptung leicht.

Hilfssatz 11. *Es ist* $-3+a_6$ *genau nur für*

$$a_6 = 3, 4, 12$$

eine Quadratzahl.

Denn aus $-3+a_6=a^2$ folgt sofort $8 \nmid a_6$, $9 \nmid a_6$, also $a_6 | 12$, ferner folgt $a_6 \geqq 3$. Hieraus entsteht die Behauptung.

Hilfssatz 12. *Es ist* $1+a_6$ *genau nur für*

$$a_6 = -9, -2, -1$$

eine Kubikzahl.

Denn aus

$$1+a_6=a^3$$

folgt $(a-1)(a^2+a+1)=a_6$, $a^2+a+1 | a_6$, also das Bestehen einer Gleichung

$$a^2+a+1=b_6.$$

Dies ergibt $(2a+1)^2=-3+4b_6$, also kommen nach Hilfssatz 11 nur

$$b_6 = 1, 3$$

in Frage. Das läßt für a nur die Möglichkeiten $a^2+a=0$ und $a^2+a=2$, d.h.

$$a = 0, -1, 1, -2$$

zu, von denen aber $a=1$ (wegen $a_6 \neq 0$) herausfällt. Hieraus und aus $a_6=-1+a^3$ folgt die Behauptung.

Hilfssatz 13. *Aus dem Bestehen von*

$$x^3-3x=1+a_6 \qquad (x \in R) \tag{75}$$

folgt das eine von $a_6 = -3, -1, 1$.

Denn die linke Seite von (75) ist gerade, also muß $2 \nmid a_6$ sein. Insbesondere für $a_6=3$ ist (75) offenbar unlösbar. Wenn somit die Behauptung falsch ist, so müßte (75) für mindestens ein a_6 mit $9 | a_6$ bestehen. Dann gälte

$$x^3-3x \equiv 1 \pmod 9.$$

Hierbei muß aber $x^3 \equiv 1 \pmod 3$, also $x \equiv 1 \pmod 3$, $x=1+3y$ $(y \in R)$ sein, woraus nach Einsetzung

$$(1+3y)^3-3(1+3y) \equiv 1 \pmod 9, \text{ d.h. } -3 \equiv 0 \pmod 9$$

folgt. Dieser Widerspruch beweist Hilfssatz 11.

Nunmehr wollen wir den Beweis von Satz 5 beenden. Zu bestimmen sind nur noch die ω_m mit Grad $\omega_m = 2$ für die natürlichen Zahlen m mit mehrfachen Primteilern. Korollar 1 liefert hierzu folgende Regel.

Man nehme die sämtlichen ω_n mit Grad $\omega_n \leqq 2$ und quadratfreiem $n(\geqq 2)$, bezeichne mit $d(\geqq 2)$ eine natürliche Zahl, deren alle Primteiler in n aufgehen, und suche die Fälle mit

$$\text{Grad } \sqrt[d]{\omega_n} = 2 \tag{76}$$

heraus; so entstehen eben die sämtlichen gewünschten ω_m in der Form

$$\omega_{dn} = \sqrt[d]{\omega_n} \tag{77}$$

Man bemerke, daß in dieser Regel nach Satz 4 und dem schon bewiesenen Teil von Satz 5 nur

$$n = 2, 3, 5, 6, 10 \tag{78}$$

in Frage kommen.

Insbesondere wenn $d = p$ $(p|n)$ ist, so kommen nur

$$d = p = 2, 3, 5 \tag{79}$$

in Betracht, aber wir zeigen vor allem. daß (76) für $p = 3, 5$ nicht befriedigt werden kann.

Denn betrachten wir zuerst den Fall

$$d = p = 3. \tag{80}$$

Nach (78) muß jetzt $n = 3$ oder 6 sein. Da nach Korollar 2 jedes ω_3 unter den $-\omega_6$ vorkommt, so genügt es (wegen Grad $\sqrt[3]{-\omega_6} =$ Grad $\sqrt[3]{\omega_6}$) unsere Behauptung für $n = 6$ zu beweisen. Wir haben auszuweisen, daß

$$\text{Grad } \sqrt[3]{\omega_6} = 2 \tag{81}$$

unmöglich ist, wenn hier für ω_6 die in den Sätzen 4, 5 aufgezählten Werte 2 und $\omega_6^{(i)}$ $(i = 1, \ldots, 6)$ eingesetzt werden.

Für $a_6 = 2$ ist das klar. Ferner besteht (81) nach Hilfssatz 7 für ein $\omega_6 = \omega_6^{(i)}$ dann und nur dann, wenn das Gleichungssystem

$$y^3 = N(\omega_6^{(i)}), \quad x^3 - 3xy = S(\omega_6^{(i)}) \qquad (x, y \in R) \tag{82}$$

lösbar ist. Nun lautet (82) (s. Satz 5) für $i = 1, \ldots, 6$ der Reihe nach als

$$(82^{(1)}) \qquad y^3 = 1 + a_6, \qquad x^3 - 3xy = 1,$$

$$(82^{(2)}) \qquad y^3 = 1, \qquad x^3 - 3xy = 1 + a_6,$$

$$(82^{(3)}) \qquad y^3 = 1 + a_6, \qquad x^3 - 3xy = 1 + a_6,$$

$$(82^{(4)}) \qquad y^3 = 1 + a_6, \qquad x^3 - 3xy = 1 - a_6,$$

$$(82^{(5)}) \qquad y^3 = 1 + 2a_6, \qquad x^3 - 3xy = 1 + a_6,$$

$$(82^{(6)}) \qquad y^3 = 1 + a_6, \qquad x^3 - 3xy = 1 + 2a_6.$$

Entsprechend unserer Behauptung werden wir zeigen, daß diese Gleichungssysteme $(82^{(i)})$ $(i=1,\ldots,6)$ jedesmal nur für solche Werte von a_6 lösbar sein können, für die das zugehörige $\omega_6^{(i)}$ entweder rational oder eine Einheitswurzel ist.

Aus dem Bestehen von $(82^{(1)})$ (sogar schon aus dem von $(82_2^{(1)})$) folgt $x|1, x^3\equiv 1 \pmod 3$, $x=1, y=0$. Hieraus und aus $(82_1^{(1)})$ folgt $a_6=-1$.

Aus $(82^{(2)})$ (sogar schon aus $(82_1^{(2)})$) folgt $y=1$. Hieraus und aus $(82_2^{(2)})$ folgt nach Hilfssatz 13 das eine von $a_6=-3, -1, 1$.

Aus $(82^{(3)})$ (sogar schon aus $(82_1^{(3)})$) folgt nach Hilfssatz 12, daß

(83) entweder $a_6=-9, y=-2$ oder $a_6=-2, y=-1$ oder $a_6=-1, y=0$

ist. Dabei geht $(82_2^{(3)})$ bzw. in

$$x^3+6x=-8,\quad x^3+3x=-1,\quad x^3=0 \tag{84}$$

über. Da hiervon nur die dritte Gleichung (in R) lösbar ist, so folgt $a_6=-1$.

Aus $(82^{(4)})$ schließt man ähnlich wie zuvor, die Abweichung ist, daß statt (84) der Reihe nach die drei Gleichungen

$$x^3+6x=10,\quad x^3+3x=3,\quad x^3=2$$

auftreten. Alle drei sind unlösbar, weshalb $(84^{(4)})$ für kein a_6 besteht.

Aus $(82^{(5)})$ (sogar schon aus $(82_1^{(5)})$) folgt nach Hilfssatz 12 $a_6=-1$.

Aus $(82^{(6)})$ schließt man ähnlich wie oben aus $(83^{(3)})$, die Abweichung ist, daß statt (84) der Reiche nach die drei Gleichungen

$$x^3+6x=-17,\quad x^3+3x=-3,\quad x^3=-1$$

auftreten. Da hiervon nur die dritte Gleichung möglich ist, so folgt wieder $a_6=-1$.

Man sieht hieraus tatsächlich, daß in den Gleichungssystemen $(82^{(i)})$ $(i=1,\ldots,6)$ jeweils nur solche a_6 möglich sind, für die das zugehörige $\omega_6^{(i)}$ entweder rational (vgl. hierzu[1])) oder eine Einheitswurzel ist. Das beweist, daß (76) im Fall (80) nicht befriedigt werden kann.

Dann haben wir den Fall

$$d=p=5 \tag{85}$$

zu betrachten. Für diesen erhalten wir das ähnliche Resultat sehr leicht. Jetzt kommen nach (78) nur $n=5$, 10 in Betracht. Da nach Korollar 2 jedes ω_5 unter den $-\omega_{10}$ vorkommt, so genügt es (wegen Grad $\sqrt[5]{-\omega_{10}}=$ Grad $\sqrt[5]{\omega_{10}}$) nur $n=10$ zu betrachten. Wir haben auszuweisen, daß

$$\text{Grad } \sqrt[5]{\omega_{10}}=2$$

nicht zutrifft, wenn für ω_{10} die Zahlen

$$\omega_{10}^{(1)} = 1 + \sqrt{-1}, \quad \omega_{10}^{(2)} = \frac{1}{2}(3 + \sqrt{3}) \tag{86}$$

aus Satz 5 eingesetzt werden. Das ist aber klar, da diese Zahlen keine 5-ten Potenzen sind. Somit haben wir bewiesen, daß (76) auch im Fall (85) nicht befriedigt werden kann.

Das bisherige bedeutet, daß die Anwendung unserer Regel unter den drei Fällen (79) nur im Fall $d = p = 2$ Zahlen von der Form (77) liefert. Freilich folgt hieraus sofort, daß in dieser Regel überhaupt unter allen d nur noch die

$$d = 2^e \qquad (e = 1, 2, \ldots) \tag{87}$$

in Betracht zu ziehen sind. Dabei kommen (unter allen Zahlen (78)) nur

$$n = 2, 6, 10 \tag{88}$$

in Frage. Diese drei Fälle betrachten wir einzeln.

Im Fall

$$n = 2 \tag{89}$$

bestimmen wir nach (77) zuerst die

$$\omega_4 = \sqrt{\omega_2}, \tag{90}$$

wobei nach (76) nur die ω_2 mit

$$\text{Grad } \sqrt{\omega_2} = 2 \tag{91}$$

zu berücksichtigen sind. Nach den Sätzen 4,5 kommen als solche nur die Zahlen

$$\omega_2 = -1 + a_2 \tag{92}$$

und

$$\omega_2 = \frac{1}{2}(-2 + a + \sqrt{a^2 + 4a_2}) \tag{93}$$

in Betracht. Für (92) ist (91) trivial erfüllt (ausgenommen wenn $-1 + a_2$ eine Quadratzahl, d.h. wenn $a_2 = 1$ oder 2 ist). Damit ferner (91) für (93) erfüllt ist, ist nach Hilfssatz 6 notwendig und hinreichend, daß das Gleichugssystem

$$y^2 = 1 - a - a_2, \quad x^2 = 2y - 2 + a \qquad (x, y \in R) \tag{94}$$

lösbar ist; selbst den Lösungen gehören dann nach demselben Hilfssatz vermöge (90) die

$$\omega_4 = \frac{1}{2}(x + \sqrt{x^2 - 4y}) \tag{95}$$

zu. Um die Lösungen von (94) zu bestimmen addieren wir die zwei Gleichungen dieses Systems:

$$x^2 + (y-1)^2 = -a_2.$$

Es genügt diese Gleichung zu lösen, da sich dann das passende a jedesmal aus (94_1) bestimmen läßt. Ihre sämtlichen Lösungen sind in der Tabelle

x	0	b_2	b_2	$-b_2$
y	$1-b_2$	1	$1-b_2$	$1-b_2$

angegeben. (Die entsprechenden Werte $-b_2^2$ bzw. $-2b_2^2$ von a_2 werden nicht gebraucht.) Werden diese x, y in (95) eingesetzt und a_2 für b_2 geschrieben, so entstehen eben die in Satz 5 mit $\omega_4^{(i)}$ $(i=1,\ldots,4)$ bezeichneten Zahlen. Da ferner die Einsetzung von (92) in (90) zu keinen neuen ω_4 (sondern wieder nur zu den $\omega_4^{(i)}$) führt, so ist hiermit Satz 5 für $n=4$ bewiesen.

Dann haben wir entsprechend dem Fall ($e=2$ d. h.) $d=4$ von (87) die ω_8 mit Grad $\omega_8=2$ zu bestimmen. Anstatt aber diese nach (77) in der Form $\omega_8=\sqrt[+]{\omega_2}$ anzusetzen, wollen wir sie auf Grund von Korollar 1 als

(96) $$\omega_8=\sqrt{\omega_4}$$

mit

(97) $$\text{Grad}\,\sqrt{\omega_4}=2$$

bestimmen, wobei die (eben bestimmten)

(98) $$\omega_4=\omega_4^{(i)} \qquad (i=1,\ldots,4)$$

aus Satz 5 in Betracht kommen. Es wird sich zeigen, daß überhaupt kein ω_8 mit Grad $\omega_8=2$ existiert, d. h. (97) für (98) nicht erfüllt ist. Wenn $i=1$ (d.h. $\omega_4=\omega_4^{(1)}=\sqrt{-1+a_4}$) ist, so ist das klar. Es bleiben die Fälle $i=2,3,4$ zu untersuchen übrig. Wegen Hilfssatz 6 haben wir zu zeigen, daß die drei Gleichungssysteme

$$y^2=N(\omega_4^{(i)}),\ x^2=2y+S(\omega_4^{(i)}) \qquad (i=2,3,4)$$

keine passenden Lösungen $x, y(\in R)$ haben. Diese Gleichungssysteme lauten (nach Satz 5) der Reihe nach als

(99) $$y^2=1, \qquad x^2=2y+a_2,$$

(100) $$y^2=1-a_2, \qquad x^2=2y+a_2,$$

(101) $$y^2=1-a_2, \qquad x^2=2y-a_2.$$

Offenbar hat (99) nur die Lösungen

$$y=1,\ x=0;\ y=1,\ x=\pm 1;\ y=1,\ x=\pm 2;\ y=-1,\ x=0,$$

ferner hat (100) nur die Lösungen

$$y=0,\ x=\pm 1,$$

endlich hat (101) überhaupt keine Lösungen. Werden nun die gefundenen

$$\frac{1}{2}(x+\sqrt{x^2-4y})$$

eingesetzt, so entstehen lauter Einheitswurzeln. Das beweist auf Grund des zweiten Teils von Hilfssatz 6 die Behauptung, daß keine ω_n mit Grad $\omega_n = 2$ existieren. Freilich folgt hieraus ähnliches für ω_{2^k} $(k \geqq 4)$ statt ω_n. Somit ist Satz 5 für $n = 2^k$ $(k \geqq 3)$ bewiesen.

Im Fall

(102) $$n = 6$$

bestimmen wir nach (77) zuerst die

(103) $$\omega_{12} = \sqrt{\omega_6},$$

wobei nach (76) nur die ω_6 mit

(104) $$\text{Grad}\sqrt{\omega_6} = 2$$

einzusetzen sind. Nach den Sätzen 4,5 kommen als solche nur die Zahlen

(105) $$\omega_6 = 2$$

und

(106) $$\omega_6 = \omega_6^{(i)} \qquad (i = 1, \ldots, 6)$$

in Betracht. Für (105) ist (104) trivial erfüllt. Damit ferner (104) für (106) erfüllt ist, ist nach Hilfssatz 6 notwendig und hinreichend, daß das Gleichungssystem

$$y^2 = N(\omega_6^{(i)}),\ x^2 = 2y + S(\omega_6^{(i)}) \qquad (x, y \in R)$$

lösbar ist. Selbst die zugehörigen ω_{12} entstehen nach Einsetzung der Lösungen x, y in

(107) $$\omega_{12} = \frac{1}{2}(x + \sqrt{x^2 - 4y}).$$

Nun handelt es sich nach Satz 5 der Reihe nach für $i = 1, \ldots, 6$ um die folgenden Gleichungssysteme:

$$\begin{aligned}
&y^2 = 1 + a_6, && x^2 = 2y + 1,\\
&y^2 = 1, && x^2 = 2y + 1 + a_6,\\
&y^2 = 1 + a_6, && x^2 = 2y + 1 + a_6,\\
&y^2 = 1 + a_6, && x^2 = 2y + 1 - a_6,\\
&y^2 = 1 + 2a_6, && x^2 = 2y + 1 - a_6,\\
&y^2 = 1 + a_6, && x^2 = 2y + 1 + 2a_6.
\end{aligned}$$

Die in Frage kommenden Werte von a_6 erhält man aus Hilfssatz 8. ausgenommen das zweite Gleichungssystem, bei dem man zu diesem Zweck der Hilfssätze 9,10 bedarf. So bekommt man leicht, daß die ersten drei Gleichungssysteme der Reihe nach nur die Lösungen

$$y = 0,\ x = \pm 1;$$

$$y = 1,\ x = 0,\ \pm 1,\ \pm 2,\ \pm 3;\ y = -1,\ x = 0,\ \pm 1;$$

$$y = 0,\ -2,\ x = 0$$

haben, dagegen die übrigen drei unlösbar sind. Die Einsetzung dieser

Lösungen in (107) liefert (Einheitswurzeln und rationale Zahlen bei Seite gelassen) die folgenden Zahlen:

$$(108) \qquad \omega_{12} = \frac{1}{2}(\pm 3 + \sqrt{5}),\ \frac{1}{2}(\pm 1 + \sqrt{5}),\ \sqrt{2}.$$

Da diese auch schon den aus (103), (105) entspringenden Fall $\omega_{12} = \sqrt{2}$ umfassen und mit den $\omega_{12}^{(i)}$ $(i = 1, 2, 3)$ in Satz 5 übereinstimmen, so ist dieser Satz für $n = 12$ bewiesen. Da ferner unter diesen Zahlen (108) nur die $\omega_{12} = \frac{1}{2}(\pm 3 + \sqrt{5})$ Quadratzahlen sind, so folgt (aus Korollar 1) auch, daß die sämtlichen ω_{24} mit Grad $\omega_{24} = 2$ die

$$(109) \qquad \omega_{24} = \sqrt{\omega_{12}} = \frac{1}{2}(\pm 1 + \sqrt{5})$$

sind. Das beweist Satz 5 für $n = 24$. Da endlich diese Zahlen (109) keine Quadratzahlen sind, so folgt ähnlich, daß keine ω_{48} mit Grad $\omega_{48} = 2$ vorhanden sind, weshalb Satz 5 für $n = 48$ richtig ist. Freilich folgt ähnliches für alle $n = 2^k 3$ $(k \geqq 5)$.

Endlich ist aus (88) nur noch der Fall

$$n = 10$$

übrig. Jetzt kommen wir ähnlich aber schnell zum Ziel. Wir betrachten die Zahlen

$$\omega_{10}^{(1)} = 1 + \sqrt{-1},\ \omega_{10}^{(2)} = \frac{1}{2}(3 + \sqrt{5})$$

aus Satz 5. Unter diesen ist nur die zweite eine Quadratzahl, weshalb die sämtlichen ω_{20} mit Grad $\omega_{20} = 2$ die

$$\omega_{20} = \sqrt{\omega_{10}^{(2)}} = \frac{1}{2}(\pm 1 + \sqrt{5})$$

sind. Das beweist Satz 5 für $n = 20$. Da endlich ω_{20} keine Quadratzahl ist, so folgt, daß keine ω_{40} mit Grad $\omega_{40} = 2$ vorhanden sind, weshalb Satz 5 für $n = 40$ richtig ist. Ähnliches folgt für alle $n = 2^k 5$ $(k \geqq 4)$. Hiermit ist der Beweis von diesem Satz beendet.

Literaturverzeichnis.

[1] L. Rédei, Potenzelemente in Körpern. (Erscheint später in den *Acta Math. Acad. Sci. Hung.*)

[2] L. Rédei, Eine Bemerkung über die endlichen einstufig nichtkommutativen Gruppen, *Acta Sci. Math.*, **19** (1958), 127—128.

[3] L. Zsigmondy, Zur Theorie der Potenzreste, *Monatshefte f. Math.*, **3** (1892), 265—284.

(Eingegangen am 1. September 1957.)