ACTA ARITHMETICA
VIII (1963)

It follows that there exists an integer k with

$$m+1 \leqslant k \leqslant m+n(3+\pi/\varkappa)$$

(consequently satisfying (2.5)) and a sequence $\varepsilon \to 0$ for which $k_\varepsilon = k$. For this sequence we get by (4.13) and by the estimation

$$\frac{e_1(\frac{1}{2}y_1 k)}{|\varrho_0|^k} > \frac{T^{1/2}e_1\left(-(\log T)^{0.9}\right)}{15^{13\log T/\log_2 T}} > T^{1/2}e_1\left(-40\frac{\log T}{\log_2 T}\right),$$

the inequality

$$S_k(\varepsilon) > T^{1/2}e_1\left(-53\frac{\log T}{\log_2 T}\right), \tag{4.14}$$

which yields on letting ε tend to zero

$$S_k \geqslant T^{1/2}e_1\left(-53\frac{\log T}{\log_2 T}\right). \tag{4.15}$$

(4.15) and (3.3) give for T sufficiently large

$$I_k \geqslant T^{1/2}e_1\left(-53\frac{\log T}{\log_2 T}\right). \tag{4.16}$$

This and the first inequality (2.7) together with (2.8) prove (1.19). (1.20) follows on an analogous way (one has to use (1.15) at (4.12) and then properly change the relations (4.13)–(4.16)).

References

[1] S. Knapowski, *On the Möbius function*, Acta Arithm. 4 (1958), pp. 209-216.

[2] — *On the mean values of certain functions in prime number theory*, Acta Math. Hung. 10 (1959), pp. 375-390.

[3] — *On sign-changes in the remainder-term in the prime number formula*, Journ. London Math. Soc. 36 (1961), pp. 451-460.

[4] — *Mean-value estimations for the Möbius function I*, Acta Arithm. 7 (1962), pp. 121-130.

[5] — *Mean-value estimations for the Möbius function II*, Acta Arithm. 7 (1962), pp. 337-343.

[6] — and P. Turán, *Comparative prime number theory III*, Acta Math. Hung. (to appear).

[7] E. C. Titchmarsh, *The theory of the zeta-function of Riemann*, Oxford 1951.

[8] P. Turán, *On some further one-sided theorems of new type in the theory of diophantine approximations*, Acta Math. Hung. 12 (1961), pp. 455-468.

Reçu par la Rédaction le 14. 1. 1963

Über die Irreduzibilität gewisser Polynome

von

I. Seres (Budapest)

In der Literatur begegnen wir uns oft mit der Irreduzibilität algebraischer Polynome von der Form

$$S(x) = F\big(R(x)\big),$$

wobei $F(z)$ ein irreduzibles Polynom mit ganzen rationalen Koeffizienten und $z = R(x)$ ein Polynom mit ebenfalls ganzen rationalen Koeffizienten bedeutet.

Der Verfasser hat sich schon in seinen früheren Arbeiten [8], [9] mit der Irreduzibilität von Polynomen eines gewissen Typs beschäftigt; als irreduzibles Polynom $F(z)$ nahm er ein beliebiges n-tes Kreisteilungspolynom $F_n(z)$, in welches er das Polynom

$$z = R(x) = \prod_{k=1}^{m}(x-a_k)Q(x) = P(x)Q(x) \tag{1}$$

substituierte, wo $a_1 < a_2 < \ldots < a_m$ ganze rationale Zahlen bedeuteten und die Koeffizienten des Polynoms

$$Q(x) = x^\mu + b_1 x^{\mu-1} + \ldots + b_\mu$$

ganze rationale Zahlen waren; der Grad von $Q(x)$ war kleiner als m.

Der Beweis der Irreduzibilität von Polynomen dieses Typs ergab die Lösung einer Verallgemeinerung eines Problems von I. Schur, [6], [3]. Für $n = 2^M$ und $Q(x) \equiv 1$ ergab sich die Irreduzibilität des Polynoms

$$S_n(x) = S_{2^M}(x) = \prod_{k=1}^{m}(x-a_k)^{2^M} + 1.$$

Es waren dabei nur einige Ausnahmen.

Im Falle $M = 0$ ist das Polynom $S_1(x)$ für spezielle gegebene $\{a_1, a_2, a_3, a_4\}$ reduzibel über dem Körper K_0 (W. Flügel [3]).

Irreduzibilität ohne Ausnahme ergab sich in den Fällen $M \geqslant 1$. (W. Flügel [4]). Für $M = 1$, $M = 2$ kann der Beweis in dem Buche von G. Pólya und G. Szegö [5] gefunden werden.

Für $M=3$ können wir den Nachweis in dem Artikel von A. Brauer, R. Brauer und H. Hopf [1] finden.

Für $M \geqslant 4$ gelang es zum ersten Male dem Verfasser einen Beweis zu finden.

Mit dem Beweis des obenerwähnten Satzes gab der Verfasser auch für den Fall der allgemeinen Kreisteilungspolynome, d. h. für

$$F_n\big(P(x)\big) = S_n(x),$$

$$\big(P(x) = \prod_{k=1}^{m}(x-a_k); \qquad m=1,2,\ldots\big)$$

in seinem Artikel [8] zusammen mit seiner ergänzenden Arbeit [9] einen Beweis. Er wies auf einen Ausnahmefall hin und zwar auf den Fall des Kreisteilungspolynoms $F_{12}(z)$, wo an die Stelle von z das Polynom $P(x) = (x-a_1)(x-a_2)(x-a_3)$ mit drei aufeinanderfolgenden ganzen rationalen Zahlen a_1, a_2, a_3 eingesetzt wurde. Genau denselben Ausnahmefall gaben für den Fall der quadratischen Körper H. L. Dorwart und O. Ore [2] an.

Der obenerwähnte Artikel [8] des Verfassers enthält auch den Beweis der Irreduzibilität folgender allgemeinerer Polynome. Bei der passender Auswahl des Polynoms $Q(x)$ braucht nicht verlangt zu werden, daß in dem Ausdruck $z = \prod_{k=1}^{m}(x-a_k)Q(x)$ die Faktoren $x-a_k$ alle mit dem Exponenten Eins vorkommen sollen. Für $R(x)$ ist die Gestalt

$$R(x) = \prod_{k=1}^{m}(x-a_k)Q(x) = (x-a_1)^{\alpha_1}(x-a_2)^{\alpha_2}\ldots(x-a_m)^{\alpha_m}Q_1(x)$$

zulässig, wobei $a_k \geqslant 1$ $(k=1,2,\ldots,m;\ m \geqslant 6)$, $Q_1(x)$ ein Polynom mit dem höchsten Koeffizienten Eins und

$$\sum_{k=1}^{m}\alpha_k + \operatorname{Grad} Q_1(x) < 2m$$

ist. Natürlich umfasst die in (1) erwähnte Wahl des Polynoms $Q(x)$ noch allgemeinere Irreduzibilitätsfälle.

Der Verfasser hat in seinem Artikel [8] mit Hilfe eines Satzes von A. V. Capelli [10] und eines sich auf die Einheiten von Kreisteilungskörpern beziehenden Satzes von L. Kronecker [4] auch gezeigt, daß das Polynom

$$T(x) = \prod_{k=1}^{m}(x-a_k) - e^{2\pi i/n} \qquad (\text{für } n \neq 12,\ n>2)$$

über dem n-ten Kreisteilungskörper K_n irreduzibel ist.

Endlich ergab sich für den Fall $m \geqslant 6$ die Irreduzibilität des Polynoms

$$U(x) = \prod_{k=1}^{m}(x-a_k)Q(x) - e^{2\pi i/n}$$

über den n-ten Kreisteilungskörper K_n (mit der Angabe des Polynoms $R(x) = \prod_{k=1}^{m}(x-a_k)Q(x)$ unter den Bedingungen des Ausdrucks (1)).

Bei dem Polynom $\prod_{k=1}^{m}(x-a_k)Q(x)$ in (1) war der Grad von $Q(x)$ kleiner als Grad $\prod_{k=1}^{m}(x-a_k)$.

Betrachten wir den Fall, in dem

$$\operatorname{Grad} Q(x) = \operatorname{Grad}\prod_{k=1}^{m}(x-a_k) = m$$

ist. Genauer, wir beweisen den folgenden

Satz I. *Es seien die ganzen rationalen Zahlen*

$$a_1 < a_2 < \ldots < a_m \qquad (m>5),$$

das n-te Kreisteilungspolynom $F_n(z)$ und das Polynom

$$Q(x) = x^{m_1} + b_1 x^{m_1-1} + \ldots + b_{m_1} \qquad (m_1 \leqslant m)$$

wobei die Koeffizienten $b_1, \ldots, b_{m_1}$ ganze rationale Zahlen sind, gegeben. Das Polynom

$$S_{n,m}(x) = F_n\Big[Q(x)\prod_{k=1}^{m}(x-a_k)\Big]$$

ist entweder irreduzibel über dem Körper der rationalen Zahlen, oder ist das Produkt von zwei über dem Körper der rationalen Zahlen irreduziblen Polynomen von gleichem Grade.

Es besteht weiter der folgende

Satz Ia. *Unter den Bedingungen des Satzes* I. *ist das Polynom*

$$T_{n,m}(x) = Q(x)\prod_{k=1}^{m}(x-a_k) - e^{2\pi i/n}$$

entweder irreduzibel über dem n-ten Kreisteilungskörper oder ist das Produkt zweier über dem n-ten Kreisteilungskörper irreduzibler gleichgradiger Polynome.

Betrachten wir die Zerlegung in Faktoren des Polynoms

$$S_{n,\mu}(x) = F_n\Big(Q(x)\prod_{k=1}^{m}(x-a_k)\Big)$$

über dem r-ten Kreisteilungskörper K_r, wo n/r und Grad $Q(x) = \mu < m$.

Wir beweisen den folgenden

SATZ II. *Es seien* $a_1 < a_2 < \ldots < a_m$ $(m \geqslant 6)$ *ganze rationale Zahlen.*

$$Q(x) = x^{\mu} + b_1 x^{\mu-1} + \ldots + b_{\mu},$$

wobei die Koeffizienten $b_1, \ldots, b_{\mu}$ *ganze rationale Zahlen sind,* $\mu = \operatorname{Grad} Q(x) < m$. *Das Polynom*

$$Q(x)\prod_{k=1}^{m}(x-a_k) - e^{2\pi i/n}$$

ist irreduzibel nicht nur über dem n*-ten Kreisteilungskörper sondern auch über dem* r*-ten Kreisteilungskörper* K_r, *wobei*

$$K_r \supset K_n .$$

Weiter haben wir den folgenden

SATZ III. *Unter den Bedingungen des Satzes* II. *ist das Polynom*

$$S_{n,\mu}(x) = F_n\Big[\prod_{k=1}^{m}(x-a_k)Q(x)\Big],$$

wobei $F_n(z)$ *das* n*-te Kreisteilungspolynom ist, über dem Körper* K_{r^*} *irreduzibel, wo* K_{r^*} *der* r^**-te Kreisteilungskörper mit der Bedingung* $(r^*, n) = 1$ *bedeutet.*

Wir werden für die Beweise der angeführten Sätze gewisse Hilfssätze nötig haben.

HILFSSATZ I. (Satz von L. Kronecker [4]). *Die Einheiten des* s*-ten Kreisteilungskörpers* K_s *haben die Gestalt*

$$\vartheta = \varepsilon\eta^l ,$$

wo ε *eine reelle Einheit aus dem Körper* K_s, l *eine ganze rationale Zahl und* η *eine Einheitswurzel ist und zwar*

1) $\eta = e^{2\pi i/s}$, *wenn* s *eine Primzahlpotenz,*

2) $\eta = e^{2\pi i/2s}$, *wenn* s *eine gerade Zahl, doch keine Primzahlpotenz,*

3) $\eta = e^{2\pi i/4s}$, *wenn* s *eine ungerade Zahl, doch keine Primzahlpotenz ist.*

HILFSSATZ II. (Spezialfall des Capelli'schen Satzes [10]): *Es seien* $F_s(z)$ *das* s*-te Kreisteilungspolynom und* $z = R(x)$ *ein Polynom mit ganzen rationalen Koeffizienten. Das Polynom*

$$S(x) = F_s\big(R(x)\big)$$

ist dann und nur dann irreduzibel über dem Körper der rationalen Zahlen, wenn das Polynom $R(x) - e^{2\pi i/s}$ *über dem* s*-ten Kreisteilungskörper irreduzibel ist.*

HILFSSATZ III. *Die Koeffizienten des Polynoms* $b(x)$ *seien ganze Zahlen aus dem* n*-ten Kreisteilungskörper* K_n. *Sind die Zahlen* a_k *und* a_l *ganz-rational und sind* $b(a_k)$ *und* $b(a_l)$ *Einheiten aus dem Körper* K_n; *gilt ferner* $|a_k - a_l| > 2$, *so haben die Vektoren* $b(a_k)$ *und* $b(a_l)$ *gleiche, oder entgegensetzte Richtungen.*

Beweis. Nach dem Hilfssatz I. läßt sich

$$b(a_k) = \eta_k \varepsilon_k , \qquad b(a_l) = \eta_l \varepsilon_l$$

setzen, wobei η_k, η_l Einheitswurzeln und $\varepsilon_k, \varepsilon_l$ reelle Einheiten (in K_n) sind. Es ist offenbar

$$(a_k - a_l)/\big(b(a_k) - b(a_l)\big) ,$$

d.h.

$$(a_k - a_l)/(\eta_k\varepsilon_k - \eta_l\varepsilon_l) ,$$

woraus man nach einer kleiner Umformung, die Beziehung

$$(a_k - a_l)/(\varepsilon_k\varepsilon_l^{-1} - \eta_k^{-1}\eta_l) \tag{3}$$

erhält.

Die Beziehung in der konjugiert komplexen Form geschrieben lautet:

$$(a_k - a_l)/(\varepsilon_k\varepsilon_l^{-1} - \eta_k\eta_l^{-1}) . \tag{4}$$

Durch Subtraktion von (3) aus (4) bekommen wir

$$(a_k - a_l)/(\eta_k\eta_l^{-1} - \eta_k^{-1}\eta_l) \tag{5}$$

und

$$|a_k - a_l|/|\eta_k\eta_l^{-1} - \eta_k^{-1}\eta_l| . \tag{6}$$

Mit anderen Worten: Ist die Summe

$$\eta_k\eta_l^{-1} - \eta_k^{-1}\eta_l \neq 0 ,$$

so ist ihr absoluter Betrag $\leqslant 2$.

Dasselbe gilt für alle Konjugierten, wogegen für die linke Seite von (6)

$$|a_k - a_l| \geqslant 3$$

gilt. Durch Normbildung (über dem rationalen Körper) entsteht

$$|N(a_k - a_l)|/|N(\eta_k\eta_l^{-1} - \eta_k^{-1}\eta_l)| . \tag{7}$$

Das ist ein Widerspruch, wenn $N(\eta_k\eta_l^{-1} - \eta_k^{-1}\eta_l) \neq 0$.

Der Widerspruch wird nicht entstehen, wenn

$$\eta_k = \pm\eta_l . \tag{8}$$

Die Vektoren $b(a_k)$ und $b(a_l)$ sind in diesem Falle unter einander parallel (oder entgegengesetzt gerichtet).

Es gilt noch der folgende

HILFSSATZ IV. *Es seien* $a_1 < a_2 < \ldots < a_m$ $(m \geqslant 6)$ *ganze rationalen Zahlen und* $b(x)$ *ein Polynom mit ganzen Koeffizienten aus dem* n*-ten Kreisteilungskörper* K_n. *Sind die Zahlen* $b(a_k)$ *für* $k = 1, 2, \ldots, m$ *Einheiten aus* K_n, *so sind die Vektoren* $b(a_k)$ *parallel.*

Beweis.

$$2 < a_4 - a_1 < a_5 - a_1 < \ldots < a_m - a_1 .$$

Hieraus und aus dem Hilfssatze III. folgt: die Vektoren $b(a_k)$ sind mit der Einheit $b(a_1)$ parallel (für $k = 4, 5, \ldots, m$). Ähnlicherweise, wegen

$$2 < a_5 - a_2 , \qquad 2 < a_6 - a_3 \tag{9}$$

sind die Vektoren $b(a_5), b(a_2)$ und $b(a_6), b(a_3)$ unter einander und nach den Obigen mit dem Vektor $b(a_1)$ parallel.

Nachbemerkung. Alle oben vorkommenden Einheiten haben nach Hilfssatz I. und IV. die folgende Gestalt:

$$b(a_k) = \pm \varepsilon_k \eta_1 , \qquad k = 1, 2, \ldots, m \geqslant 6 , \tag{10}$$

wobei ε_k eine reelle Einheit und η_1 eine Einheitswurzel ist.

HILFSSATZ V. *Das Polynom von folgender Gestalt:*

$$R(x) - e^{2\pi i l/n}$$

wo $R(x)$ *ein reelles Polynom und* $e^{2\pi i l/n}$ *eine (komplexe) Einheitswurzel ist, hat keinen reellen Polynomteiler.*

Beweis. Ist das reelle Polynom $g(x)$ ein Teiler von $R(x) - e^{2\pi i l/n}$, so geht das reelle Polynom $g(x)$ in $R(x)$ nicht auf, und wenn wir die Division von $R(x)$ durch $g(x)$ durchführen, so erhalten wir

$$R(x) = g(x) W(x) + r(x) .$$

Die hier aufgeschriebene Polynome haben alle reelle Koeffizienten und es ist offenbar, daß $\operatorname{Grad}(r(x)) < \operatorname{Grad}(g(x))$ ist. Einerseits ist $R(x) - e^{2\pi i l/n} \equiv o \,(\operatorname{mod} g(x))$, andererseits

$$R(x) - e^{2\pi i l/n} \equiv r(x) - e^{2\pi i l/n} \equiv 0 \,(\operatorname{mod} g(x)) .$$

Die letzte Kongruenz kann aber nicht bestehen, da die Koeffizienten von $r(x)$ reell sind und $e^{2\pi i l/n}$ eine komplexe Zahl ist, und die Bezeihung

$$\operatorname{Grad}\left(r(x) - e^{2\pi i l/n}\right) < \operatorname{Grad} g(x)$$

gilt.

Beweis des Satzes I. Nehmen wir an, daß das Polynom

$$S_{n,m}(x) = F_n\Big[Q(x) \prod_{k=1}^{m} (x - a_k)\Big]$$

über dem Körper der rationalen Zahlen reduzibel ist. In diesem Falle ist laut Hilfssatz II. das Polynom

$$T(x) = Q(x) \prod_{k=1}^{m} (x - a_k) - e^{2\pi i/n}$$

reduzibel über K_n:

$$T(x) = Q(x) \prod_{k=1}^{m} (x - a_k) - e^{2\pi i/n} = g(x) h(x) . \tag{11}$$

Ohne Einschränkung der Allgemeinheit können wir annehmen, daß $g(x)$ ein Polynomfaktor von $T(x)$ kleinsten Grades mit dem höchsten Koeffizienten 1 ist.

Das Polynom $T(x)$ hat auch den höchsten Koeffizienten 1 und die übrigen Koeffizienten sind ganze Zahlen aus dem Körper K_n, infolge dessen sind die Koeffizienten von $g(x)$ und $h(x)$ ganze Zahlen aus dem Körper K_n. Nun behaupten wir, daß die Annahme

$$0 < \operatorname{Grad} g(x) < m \tag{12}$$

zu einem Widerspruch führt. Die Zahlen $g(a_k)$ $(k = 1, 2, \ldots, m)$ sind Einheiten aus dem Kreisteilungskörper K_n.

Nämlich nach (11)

$$g(a_k) h(a_k) = -e^{2\pi i/n}$$

und $g(a_k)$, $h(a_k)$ sind ganze Zahlen und $e^{2\pi i/n}$ ist eine n-te Einheitswurzel.

Nach der Bemerkung des Hilfssatzes IV. haben die Zahlen $g(a_k)$ folgende Gestalt

$$g(a_k) = \pm \varepsilon_k \eta_1 \qquad (k = 1, 2, \ldots, m \ (\geqslant 6)) .$$

Das Polynom $g(x)$ erfüllt nämlich die Bedingungen des Hilfssatzes IV.

Mit Hilfe der Lagrange'schen Interpolationsformel bekommen wir für

$$g(x) = \eta_1 \sum_{k=1}^{\gamma+1} \frac{P_1(x)(\pm \varepsilon_k)}{P_1'(a_k)(x - a_k)} = \eta_1 L_{\gamma+1}(x) ,$$

wo $P_1(x) = \prod_{k=1}^{\gamma+1} (x - a_k)$ und $L_{\gamma+1}(x)$ ein Polynom mit reellen Koeffizienten und γ der Grad von $g(x)$ ist.

Da wir angenommen haben, daß das Polynom $g(x)$ den höchsten Koeffizienten 1 hat, so ist $\eta_1 = \pm 1$.

Auch $g(x)$ ist ein Polynom mit reellen Koeffizienten. Das ergibt nach dem Hilfssatz V. einen Widerspruch.

Die Ursache des Widerspruchs ist, daß wir *den Grad* des irreduziblen *Faktors* $g(x)$ von $T(x)$ *größer als* 0 *und kleiner als* m *angenommen haben.*

Dieser Widerspruch verschwindet, wenn

1) $g(x)$ gleich einer Konstanten ist, dann ist $T(x)$ irreduzibel über K_n; dies gilt für jedes Konjugierte von $T(x)$ und nach dem Hilfssatz II. gilt auch für

$$S_{n,m}(x) = F_n\Big[\prod_{k=1}^{m}(x-a_k)Q(x)\Big]$$

über dem rationalen Zahlkörper.

2) (Die zweite Möglichkeit):

$$\mathrm{Grad}\, g(x) = m = \mathrm{Grad}\, h(x)$$

ist. Ähnliches gilt auch für $S_{n,m}(x)$. Damit ist der Satz I. bewiesen.

Nachbemerkungen.

1) Der Verfasser hatte bewiesen [9], daß *das Polynom*

$$F_n\Big(\prod_{k=1}^{m}(x-a_k)\Big) = S_n(x)$$

über dem rationalen Zahlkörper irreduzibel ist, falls die Anzahl (m) *der gegebenen rationalen Zahlen* (a_k) *nicht kleiner als* 5 *ist.*

Der Beweis dieser Behauptung ist, wie folgt:

A) Nach dem Hilfssatz II. ist die Reduzibilität von $S_n(x)$ äquivalent $(Q(x) \equiv 1)$ mit der Reduzibilität von

$$T(x) = \prod_{k=1}^{m}(x-a_k) - e^{2\pi i/n},$$

d.h. mit der Möglichkeit der Zerlegung

$$T(x) = g(x)h(x) \quad \text{über} \quad K_n, \tag{13}$$

wo der Grad des irreduziblen Polynoms $g(x)$ kleiner als m ist. Die Gültigkeit der Annahme $0 < \mathrm{Grad}\, g(x) < m$ $(m \geqslant 6)$ gestattet jedoch eine solche Zerlegung in Faktoren nicht.

Im Falle $m = 5$ hat ein Faktor $g(x)$ von $T(x)$ den Grad $\leqslant 2$. Nach geeigneter Wahl der Interpolationsknotenpunkte können wir das Polynom $g(x)$ konstruieren. Nämlich, wegen

$$a_5 - a_1 > a_4 - a_1 > 2$$

werden die Vektoren $g(a_1)$, $g(a_5)$, $g(a_4)$ nach der Bemerkung zum Hilfssatz IV. parallel:

$$g(a_1) = \varepsilon_1\eta_1, \quad g(a_5) = \pm\varepsilon_5\eta_1, \quad g(a_4) = \pm\varepsilon_4\eta_1$$

und das Polynom $g(x) = \pm\eta_1 L(x)$.

Hier ist die Beziehung $\eta_1 = \pm 1$ auch notwendig, wenn das Polynom $g(x)$ den höchsten Koeffizienten Eins besitzt. Nach Hilfssatz V. ist ein solcher Polynomfaktor nicht zulässig.

B) Nun untersuchen wir die Zerlegung des Polynoms

$$F_n\Big(\prod_{k=1}^{m}(x-a_k)\Big),$$

wenn die Anzahl der Faktoren von $\prod_{k=1}^{m}(x-a_k)$ kleiner als 5 ist. Zu diesem Zwecke haben wir eine Ergänzung des Hilfssatzes III. nötig.

Hilfssatz III. A. *Es seien die Koeffizienten des Polynoms* $b(x)$ *ganze Zahlen aus dem* n*-ten Kreisteilungskörper* K_n. *Sind die Zahlen* a_k *und* a_l *ganz rational und sind* $b(a_k)$ *und* $b(a_l)$ *Einheiten, gilt ferner* $|a_k - a_l| = 2$, *so gilt für die Vektoren* $b(a_k)$ *und* $b(a_l)$ *der folgende Zusammenhang*

$$b(a_k) = i^a b(a_l),$$

wo die Zahl a *ganz rational ist.*

Beweis. Nach der Beziehung (7) von Hilfssatz III. erhalten wir

$$|N(a_k - a_l)| = N(2)/|N(\eta_k\eta_l^{-1} - \eta_k^{-1}\eta_l)|, \tag{7'}$$

d.h.

$$N(2) = 2^t/|N(\eta_k\eta_l^{-1} - \eta_k^{-1}\eta_l)|. \tag{7''}$$

Es gibt zwei Möglichkeiten:

Die erste Möglichkeiten erhalten wir im Falle

$$2^t/|N(\eta_k\eta_l^{-1} - \eta_k^{-1}\eta_l)|.$$

Diese Teilbarkeit ist nur dann möglich, wenn

$$N(\eta_k\eta_l^{-1} - \eta_k^{-1}\eta_l) = 0. \tag{14}$$

Das bedeutet, daß $\eta_k = \pm\eta_l$.

Die zweite Möglichkeit bekommen wir im Falle

$$N(2)/|N(\eta_k\eta_l^{-1} - \eta_k^{-1}\eta_l)| = N(2).$$

Die Beziehung

$$N(2) = |N(\eta_k\eta_l^{-1} - \eta_k^{-1}\eta_l)|$$

gilt dann und nur dann, wenn der Betrag von $\eta_k\eta_l^{-1} - \eta_k^{-1}\eta_l$ gleich dem Betrag seiner Konjugierten und $= 2$ ist:

$$|\eta_k\eta_l^{-1} - \eta_k^{-1}\eta_l| = 2.$$

Es gilt noch die Beziehung

$$|\eta_k\eta_l^{-1}| + |-\eta_k^{-1}\eta_l| = 2.$$

Diese zwei Gleichungen bedeuten, daß die drei Vektoren $\eta_k\eta_l^{-1}$, $-\eta_k^{-1}\eta_l$ und $\eta_k\eta_l^{-1}-\eta_k^{-1}\eta_l$ auf einer Geraden liegen.

Endlich erhalten wir

$$\eta_l^{-1}\eta_k = -\eta_k^{-1}\eta_l ,$$

mit anderen Worten

$$\eta_k = \pm i\eta_l .$$

Damit ist der Hilfssatz III. A. bewiesen.

Nun setzen wir die Untersuchung der Zerlegung des Polynoms

$$F_n\Big(\prod_{k=1}^{m}(x-a_k)\Big),$$

wo $a_1 < a_2 < a_3 < a_4$ ganze rationale Zahlen mit möglichst kleinsten absoluten Beträgen sind, fort.

Es seien wieder $F_n(z)$ das n-te Kreisteilungspolynom und $m = 4, 3, 2$ oder 1.

(Die Annahme, daß die Zahlen a_k möglichst kleinste Beträge haben sollen, bedeutet keine Einschränkung. Durch Ersetzen von a_k durch a_k+a erreichen wir die möglichst kleinsten Zahlen, wobei a eine geeignete ganze rationale Zahl ist.)

Laut Hilfssatz II. genügt es die eventuelle Zerlegung des Polynoms

$$T(x) = \prod_{k=1}^{m}(x-a_k) - e^{2\pi i/n}$$

zu untersuchen.

Im Falle $m = 4$ gilt der folgende

Satz III_4. *Das Polynom*

$$\prod_{k=1}^{4}(x-a_k) - e^{2\pi i/n}$$

ist über dem n-ten Kreisteilungskörper irreduzibel, wenn $a_1 < a_2 < a_3 < a_4$ ganze rationale Zahlen sind.

Beweis. Nehmen wir an, daß das Polynom $T(x)$ über dem Körper K_n reduzibel ist

$$T(x) = g(x)h(x) ,$$

wo $g(x)$ ein irreduzibles Polynom von kleinsten Grade, mit dem höchsten Koeffizienten 1 (und sonst mit ganzen Koeffizienten aus dem Körper K_n) ist:

$$\mathrm{Grad}\, g(x) \leqslant 2 .$$

Wir wollen das Polynom $g(x)$ mit Hilfe der Lagrange'schen Interpolationsformel herstellen. Wählen wir zu diesem Zwecke drei Knotenpunkte a_1, a_4, a_r ($r = 2$ oder 3). Die zugehörigen Funktionswerte seien

$$g(a_1),\ g(a_4),\ g(a_r) .$$

Die Zahlen $g(a_k)$ $(k = 1, 2, 3, 4)$ sind Einheiten. Laut des ersten Hilfssatzes haben sie die Form

$$g(a_k) = \varepsilon_k\eta_k ,$$

wo η_k Einheitswurzeln und ε_k reelle Einheiten sind.

Es gibt zwei Möglichkeiten

(15) (A) $\qquad a_4 - a_1 \geqslant 4 ,$

(16) (B) $\qquad a_4 - a_1 = 3 .$

Im Falle (A) unterscheiden wir drei Fälle

$$\text{(a) } a_2-a_1 = 1, \quad \text{(b) } a_2-a_1 = 2, \quad \text{(c) } a_2-a_1 > 2 .$$

(17) (A.a) Ist $a_2-a_1 = 1$, so ist $a_4-a_2 = (a_4-a_1)-(a_2-a_1) \geqslant 4-1 = 3$.

(18) (A.b) Ist $a_2-a_1 = 2$, dann ist $a_3-a_1 > 2$.

Wir erhalten nach Hilfssatz III.:

Im Falle (A.a) mit Berücksichtigung der Ungleichungen (15) und (17)

$$\eta_4 = \pm\eta_1 , \quad \eta_4 = \pm\eta_2 \ (= +\eta_1) .$$

Im Falle (A.b) mit Beachtung der Ungleichungen (15) und (18) erhalten wir

$$\eta_4 = \pm\eta_1 , \quad \eta_3 = \pm\eta_1 .$$

Im Falle (A.c) mit Rücksichtnahme auf die Ungleichungen $a_4-a_1 > 2$ und $a_2-a_1 > 2$ bekommen wir

$$\eta_4 = \pm\eta_1 , \quad \eta_2 = \pm\eta_1 .$$

Demzufolge kommen wir zu dem Resultat, daß die Einheiten $g(a_1)$, $g(a_4)$ und $g(a_r)$ untereinander parallel sind (wobei $r = 2$ in dem Fällen (A.a) und (A.c) $r = 3$ in dem Falle (A.b) ist).

Die Interpolationsformel ergibt das Polynom

$$g(x) = \eta_1 \sum_{\substack{k=1\\k=4\\k=r}} \frac{P_1(x)(\pm\varepsilon_k)}{P_1'(a)(x-a_k)} ,$$

$$P_1(x) = (x-a_1)(x-a_4)(x-a_r) .$$

Der Koeffizientenvergleich ergibt, daß $\eta_1 = \pm 1$ und daß das Polynom $g(x)$ lauter reelle Koeffizienten hat.

Nach Hilfssatz V. gelangen wir somit zu einem Widerspruch.

Untersuchen wir *die möglichen Fälle von* (B). Ohne Einschränkung der Allgemeinheit können wir annehmen, daß

$$a_1 = 0, \quad a_2 = 1, \quad a_3 = 2, \quad a_4 = 3 .$$

Es gibt zwei Möglichkeiten:

(B.a) $\quad \mathrm{Grad}\, g(x) = 1\,,$

(B.b) $\quad \mathrm{Grad}\, g(x) = 2\,.$

Der Fall (B.a) ist einfach. Die Interpolationsknoten a_1 und a_4 sind hier zu gebrauchen. Nämlich

$$a_4 - a_1 > 2\,.$$

Nach den Hilfssätze I., IV. und V. gelangen wir zu einen Widerspruch.

Der Fall (B.b) ist ein wenig komplizierter. Nehmen wir an, daß das Polynom $g(x) = x^2 + Ax + B$ und das Polynom $h(x) = x^2 + Cx + D$ ist.

Es gilt folgende Identität:

$$g(1) - g(2) + \frac{g(3) - g(0)}{3} = 0\,.$$

Nach dem ersten Hilfssatz ist

$$\varepsilon_2 \eta_2 - \varepsilon_3 \eta_3 + \frac{\varepsilon_4 \eta_4 - \varepsilon_1 \eta_1}{3} = 0\,. \tag{19}$$

Die Einheiten

$$\begin{aligned} g(3) &= \varepsilon_4 \eta_4 = g(a_4)\,, \\ g(0) &= \varepsilon_1 \eta_1 = g(a_1) \end{aligned} \tag{20}$$

sind miteinander parallel, was aus der Ungleichung $|a_4 - a_1| > 2$ nach dem Hilfssätze III. folgt. Nun haben wir die Differenz $a_3 - a_1 = 2$. Nach dem Hilfssatz III. A. ist entweder

(B.b.1) $\quad \mathrm{Norm}(\eta_1 \eta_3^{-1} - \eta_1^{-1} \eta_3) = 0\,,$

oder

(B.b.2) $\quad \mathrm{Norm}(\eta_1 \eta_3^{-1} - \eta_1^{-1} \eta_3) = 2\,.$

Im Falle (B.b.1) ist

$$\eta_1 = \pm \eta_3\,. \tag{21}$$

Nach den Beziehungen (20), (21) sind die Einheiten $g(a_1), g(a_4), g(a_3)$ unter einander parallel, d.h., $g(x)$ ist ein Polynom mit reellen Koeffizienten.

Nach den Hilfssätzen IV., V. bedeutet dies einen Widerspruch.

Im Falle (B.b.2) haben wir die Gleichung

$$\begin{aligned} \eta_3 &= i^{2a_1+1} \eta_1\,, \\ \eta_2 &= i^{2a_3+1} \eta_4 \end{aligned} \tag{22}$$

und

$$\eta_4 = \pm \eta_1\,.$$

Die ersten beiden Gleichungen (22) folgen nach Hilfssatz III. A. aus $a_3 - a_1 = 2$, bzw. $a_4 - a_2 = 2$, die dritte Gleichung folgt laut Hilfssatz III. aus $a_4 - a_1 = 3$.

Es gilt noch die Identität

$$g(a_2) - g(a_3) + \frac{g(a_4) - g(a_1)}{3} = 0\,,$$

d.h. (nach Hilfssatz I.)

$$\eta_2 \varepsilon_2 - \eta_3 \varepsilon_3 + \frac{\eta_4 \varepsilon_4 - \eta_1 \varepsilon_1}{3} = 0$$

und laut (22)

$$i^{2a_3+1} \varepsilon_2 \eta_1 - i^{2a_1+1} \varepsilon_3 \eta_1 + \frac{\pm \varepsilon_4 - \varepsilon_1}{3} = 0\,.$$

Dividieren wir diese Gleichung durch η_1. Der reelle und der imaginäre Teil dieser Gleichungen sind gleich 0, d.h.

$$g(a_2) = g(a_3) \quad \text{und} \quad g(a_4) = g(a_1)\,.$$

Aus der letzten erhalten wir

$$g(3) = g(0)\,.$$

Kehren wir zu der Gleichung $g(x) = x^2 + Ax + B$ zurück. Es ist $9 + 3A + B = B$, d.h. $A = -3$.

In ähnlicher Weise erhalten wir für den Koeffizienten von $h(x)$ $C = -3$.

Vergleichen wir die entsprechenden Koeffizienten auf den beiden Seiten der Gleichung

$$x(x-1)(x-2)(x-3) - e^{2\pi i/n} = g(x)h(x) = (x^2 - 3x + B)(x^2 - 3x + D)\,.$$

Wir erhalten

$$B + D = 2 \quad \text{und} \quad BD = -e^{2\pi i/n} = \xi\,, \tag{23}$$

d.h.

$$B = 1 \pm \sqrt{1+\xi} \quad \text{und} \quad D = 1 \mp \sqrt{1+\xi}\,.$$

Die B und D sind ganze Zahlen und Einheiten. Eine dieser Einheiten (nach (23)) hat die Gestalt $1 + \sqrt{1+\xi}$ was nach dem ersten Hilfssatz einen Widerspruch bedeutet; nämlich

$$\arc \xi = \frac{2\pi}{n}\,, \quad \arc(1+\xi) = \frac{2\pi}{2n}\,, \quad \arc \sqrt{1+\xi} = \frac{2\pi}{4n}\,, \quad \arc\left(1 + \sqrt{1+\xi}\right) < \frac{2\pi}{4n}\,.$$

Eine solche Einheit gibt es in dem n-ten Kreisteilungskörper nicht. Damit ist der Fall $m = 4$ erledigt; das Polynom

$$F_n\left(\prod_{k=1}^{4} (x - a_k)\right)\,, \quad n > 2$$

ist irreduzibel.

Der Fall $m=3$.

SATZ IV. *Es seien $a_1<a_2<a_3$ ganze rationale Zahlen und $F_n(z)$ das n-te Kreisteilungspolynom; ferner sei $P(x)=(x-a_1)(x-a_2)(x-a_3)$ gesetzt. Das Polynom*

$$F_n(P(x))$$

ist über dem Körper der rationalen Zahlen K_0, dann und nur dann reduzibel, wenn a_1, a_2, a_3 drei aufeinander folgende ganze Zahlen sind und

$$n=12, \quad d.h. \quad F_{12}(z)=z^4-z^2+1 .$$

Noch allgemeiner ist der

SATZ IV.a. *Es sei $P(x)=(x-a_1)(x-a_2)(x-a_3)$, wo $a_1<a_2<a_3$ ganze rational sind. Das Polynom*

$$T(x)=P(x)-e^{2\pi il/n}, \quad (l,n)=1$$

ist dann und nur dann reduzibel über dem Körper K_n, wenn a_1, a_2, a_3 drei aufeinanderfolgende ganze rationale Zahlen sind und der Körper K_n der zwölfte Kreisteilungskörper ist.

Beweis von IV.a. Nach dem Hilfssatz II. genügt es die eventuelle Zerlegung des Polynoms

$$T(x)=P(x)-e^{2\pi i/n}$$

in Faktoren über dem Körper K_n zu untersuchen.

Nehmen wir an, daß das Polynom $T(x)=(x-a_1)(x-a_2)(x-a_3)-e^{2\pi i/n}$ über dem Körper K_n reduzibel; $=g(x)h(x)$ sei. Der Grad von $g(x)$ ist gleich Eins und somit sind $g(x)$ und $h(x)$ von der Form $g(x)=x+A$, $h(x)=x^2+Bx+C$.

Die Zahlen $g(a_k)$ sind hier auch Einheiten und sind von der Form

$$g(a_k)=\varepsilon_k\eta_k \qquad (k=1,2,3),$$

wobei die ε_k reelle Einheiten, und die η_k Einheitswurzeln sind.

Genau zwei Fälle sind möglich: $a_3-a_1>2$, $a_3-a_1=2$ $(a_3-a_1>1)$.

1) Im Falle $a_3-a_1>2$ ist das Polynom

$$T(x)=\prod_{k=1}^{3}(x-a_k)-e^{2\pi i/n}$$

über dem Körper K_n irreduzibel.

Dies folgt aus den Hilfssätzen III., IV. und V. (und aus der Interpolationsformel für $g(x)$).

2) Es sei $a_3-a_1=2$. Ohne Einschränkung der Allgemeinheit können wir annehmen, daß $a_1=-1$, $a_2=0$, $a_3=1$ sind.

Nach dem Hilfssatz III. A. haben wir die folgenden Beziehungen für die Einheiten

$$g(a_1)=\varepsilon_1\eta_1, \qquad g(a_3)=\varepsilon_3\eta_3$$

und zwar

$$\eta_3=\pm\eta_1 i^{\alpha} \qquad (\alpha=0,1,2,3). \tag{24}$$

2a) Wenn α eine gerade Zahl ist, so ist $\eta_3=\pm\eta_1$ und die Hilfssätze IV. und V. zeigen, daß die Konstruktion des reellen Polynoms $g(x)$ undurchführbar ist.

2b) Wenn α eine ungerade Zahl ist $(\alpha=2\beta+1)$, dann ist

$$g(-1)=-1+A=\varepsilon_1\eta_1,$$
$$g(1)=1+A=\varepsilon_3\eta_3$$

und nach (24)

$$\varepsilon_1\eta_1+1=A=\frac{\varepsilon_1\eta_1+\varepsilon_3\eta_3}{2}=\frac{\varepsilon_1+\varepsilon_3 i^{2\beta+1}}{2}\eta_1 . \tag{25}$$

Aus dieser Gleichung können wir die Einheitswurzel $-\eta_1^{-1}$ ausdrücken:

$$-\eta_1^{-1}=\frac{\varepsilon_1-\varepsilon_3 i^{2\beta+1}}{2}$$

und ihre konjugiert Komplexe ist

$$-\eta_1=\frac{\varepsilon_1+\varepsilon_3 i^{2\beta+1}}{2} .$$

Setzen wir diese Größe in die Gleichung (25) ein, so erhalten wir

$$A=-\eta_1^2 \quad \text{und} \quad g(x)=x-\eta_1^2 . \tag{25a}$$

Die Koeffizientenvergleich in den Gleichungen

$$\begin{aligned} P(x)-e^{2\pi i/n} &= x(x-1)(x+1)-e^{2\pi i/n}=x^3-x-e^{2\pi i/n} \\ &= g(x)h(x)=(x-\eta_1^2)(x^2+Bx+C) \\ &= x^3+(-\eta_1^2+B)x^2+(-B\eta_1^2+C)x-C\eta_1^2 \end{aligned}$$

ergibt das Gleichungssystem:

$$\begin{aligned} -\eta_1^2+B&=0, \\ -B\eta_1^2+C&=1, \\ -C\eta_1^2&=-e^{2\pi i/n} . \end{aligned} \tag{26}$$

Nach Eliminierung von B und C bekommen wir

$$-\eta_1^6+\eta_1^2+e^{2\pi i/n}=0 . \tag{27}$$

Der absolute Betrag der Glieder $-\eta_1^6$ und η_1^2 ist Eins:

$$|-\eta_1^6|=|\eta_1^2|=|e^{2\pi i/n}|=1 . \tag{27a}$$

Aus den Gleichungen (27) und (27a) bekommen wir, daß die Vektoren

$$-\eta_1^6, \quad \eta_1^2, \quad e^{2\pi i/n}$$

ein gleichseitiges Dreieck bilden, d.h.

$$\eta_1^2 = e^{\pm 2\pi i/3} e^{2\pi i/n}. \tag{28}$$

Die dritte Potenz der beiden Seiten bestimmt die Beziehung

$$-\eta_1^6 = -e^{3(2\pi i/n)}. \tag{29}$$

Setzen wir diese letzten Werte aus der Beziehung (28) und (29) in die Gleichung (27) ein, so bekommen wir die Gleichung

$$-e^{(2\pi i/n)\cdot 3} + e^{2\pi i/n} e^{\pm(2\pi i/3)} + e^{2\pi i/n} = 0$$

und nach Division durch $e^{2\pi i/n}$ $(\neq 0)$,

$$(e^{2\pi i/n})^2 = 1 + e^{\pm(2\pi i/3)} = \begin{cases} \frac{1}{2} + i\frac{\sqrt{3}}{2} = e^{2\pi i/6}, \\ \frac{1}{2} - i\frac{\sqrt{3}}{2} = e^{(2\pi i/6)\cdot 5}. \end{cases}$$

Die Zahlen

$$e^{2\pi i/n} = \pm e^{2\pi i/12}, \quad e^{2\pi i/n} = \pm e^{(2\pi i/12)\cdot 5} \tag{30}$$

sind die vier 12-te primitive Einheitswurzeln.

Nehmen wir zuerst die erste Wurzel

$$e^{2\pi i/n} = e^{2\pi i/12}$$

und setzen wir den Wert $e^{2\pi i/12}$ in die Gleichung (28) ein, so bekommen wir die Beziehung

$$\eta_1^2 = e^{10\pi i/12} \quad \text{(oder } \eta_1^2 = -i\text{)}. \tag{28a}$$

Nach (25a) ist $A = -e^{10\pi i/12}$ und wir haben endlich die Gleichung $(g(x) = x + A$, oder)

$$g(x) = x - e^{10\pi i/12}.$$

(Der andere Wert von η_1^2 $(= -i)$ ist unbrauchbar. Das Polynom $P(x) - e^{2\pi i/12} = x(x-1)(x+1) - e^{2\pi i/12}$ hat keinen Teiler von der Form $g(x) = x + i$.)

Aus dem Gleichungssystem (26) bekommen wir die Koeffizienten $B = e^{10\pi i/12}$, $C = e^{16\pi i/12}$ und die Gleichung $h(x) = x^2 + Bx + C$ wird so aussehen:

$$h(x) = x^2 + e^{10\pi i/12} x + e^{16\pi i/12},$$

und zuletzt erhalten wir die Zerlegung des Polynoms

$$T(x) = (x+1)x(x-1) - e^{2\pi i/12} = (x - e^{10\pi i/12})(x^2 + e^{10\pi i/12} x + e^{16\pi i/12}). \tag{31}$$

Das Polynom $T(x) = x^3 - x - e^{2\pi i/12}$ ist über dem Kreisteilungskörper K_{12} reduzibel, also ist das Polynom (nach dem Hilfssatz II.)

$$F_{12}(P(x)) = P^4(x) - P^2(x) + 1,$$

wo

$$P(x) = (x+1)x(x-1) = x^3 - x$$

über dem rationalen Zahlkörper reduzibel:

$$F_{12}(P(x)) = \operatorname{Norm} g(x) \cdot \operatorname{Norm} h(x) = (x^4 - x^2 + 1)(x^8 - 3x^6 + 2x^4 + 1).$$

H. L. Dorwart und Oystein Ore [2] haben über dem quadratischen Zahlkörper dieselbe Zerlegung erhalten.

Wir bekommen noch allgemeinere zerlegbare Polynome durch die Substitution: $(x \to x + a)$ (a ganz rational).

Durch Anwendung der Galois'schen Theorie erhalten wir aus dem Polynomzerlegung von $T(x)$ durch den Gebrauch der Substitutionen

$$(e^{2\pi i/12} \to e^{(2\pi i/12)\cdot 5}), \quad (e^{2\pi i/12} \to e^{(2\pi i/12)\cdot 7}), \quad (e^{2\pi i/12} \to e^{(2\pi i/12)\cdot 11})$$

die übrigen, mit $T(x)$ automorphen Polynome, und ihre Zerlegungen

$$x^3 - x - e^{10\pi i/12} = (x - e^{2\pi i/12})(x^2 + e^{2\pi i/12} x + e^{8\pi i/12}),$$
$$x^3 - x - e^{14\pi i/12} = (x - e^{22\pi i/12})(x^2 + e^{22\pi i/12} x + e^{16\pi i/12}),$$
$$x^3 - x - e^{22\pi i/12} = (x - e^{14\pi i/12})(x^2 + e^{14\pi i/12} x + e^{8\pi i/12}).$$

Damit sind alle möglichen Zerlegungen der betrachteten Art über dem zwölften Kreisteilungskörper angeführt.

Der Fall $m = 2$ $(n > 2)$.

Satz V. *Das Polynom*

$$F_n((x-a_1)(x-a_2)) = S_{n,2}(x) \qquad (n > 2)$$

ist über dem rationalen Zahlkörper K_0 irreduzibel ($a_1 < a_2$ *zwei ganze rationale Zahlen*).

Beweis. Nach dem Hilfssatz II. untersuchen wir die eventuelle Zerlegung des Polynoms

$$T(x) = (x-a_1)(x-a_2) - e^{2\pi i/n} = g(x)h(x) = (x+A)(x+B); \qquad g(x) = x + A$$

über K_n.

1) Ist $a_2 - a_1 > 2$ so ist, wie wir es gesehen haben, das Polynom $S_{n,2}(x)$ über dem Körper K_0 irreduzibel. (Dies folgt aus den Hilfssätzen I., III. und V. Wir können nämlich nur einen reellen linearen Polynomfaktor von $T(x)$ konstruieren, was einen Widerspruch bedeutet.)

2) Es sei $a_2 - a_1 = 2$. Ohne Einschränkung der Allgemeinheit nehmen wir an, daß $a_1 = -1$, $a_2 = 1$ ist. Nach dem Hilfssatze III. A. ist

$$\arg g(a_2) = \arg g(a_1) + \alpha\frac{\pi}{2} \qquad (\alpha = 0, 1, 2, 3).$$

A) Im Falle $a=0$ (oder 2) sind die Vektoren $g(a_1)$ und $g(a_2)$ miteinander parallel. Die Hilfssätze IV., V. führen zu einem Widerspruch.

B) Im Falle $a=2\beta+1$ haben wir die Gleichungen

$$\begin{aligned} g(a_1) &= -1+A = \varepsilon_1\eta_1\,, \\ g(a_2) &= 1+A = \varepsilon_2 i^{2\beta+1}\eta_1 = \varepsilon_2\eta_2 \end{aligned} \tag{32}$$

(s. Hilfssatz III. A.; die Einheiten $\varepsilon_1, \varepsilon_2$ sind reell und die η_1, η_2 sind Einheitswurzeln).

Nach (32) haben wir

$$A = \frac{\varepsilon_1 + i^{2\beta+1}\varepsilon_2}{2}\eta_1\,, \qquad -\eta_1^{-1} = \frac{\varepsilon_1 - i^{2\beta+1}\varepsilon_2}{2}$$

(und $-\eta_1 = \dfrac{\varepsilon_1 + i^{2\beta+1}\varepsilon_2}{2}$ hämlich die ε_1 und ε_2 sind reelle Zahlen).

Hieraus: $A=-\eta_1^2$ und $g(x)=x-\eta_1^2$, ähnlicherweise ist $h(x)=x-\eta_2^2$.

Aus dem Koeffizientenvergleich in der Gleichung

$$(x-a_1)(x-a_2)-e^{2\pi i/n} = (x-\eta_1^2)(x-\eta_2^2)$$

bekommen wir, daß $(a_1=-1,\ a_2=1)$

$$a_1+a_2 = 0 = \eta_1^2+\eta_2^2\,, \qquad -1-e^{2\pi i/n} = \eta_1^2\eta_2^2\,. \tag{32'}$$

Aus diesem Gleichungssystem bekommen wir

$$\eta = \sqrt[4]{1+e^{2\pi i/n}}, \qquad \arg e^{2\pi i/n} = \frac{2\pi}{n}, \qquad \arg(1+e^{2\pi i/n}) = \frac{2\pi}{2n},$$

$$\arg\eta \arg\sqrt[4]{1+e^{2\pi i/n}} = \frac{2\pi(1+2ns)}{8n} \qquad (s=0,1,2,3)\,.$$

Nach dem ersten Hilfssatz kann $\arg\eta$ nicht gleich einem ungeraden Vielfachen von $2\pi/8$ sein.

3) $a_2-a_1=1$. Es sei $a_1=-1,\ a_2=0$

$$P(x)-e^{2\pi i/n} = (x+1)x-e^{2\pi i/n} = x^2+x-e^{2\pi i/n},$$

in Wurzelfaktorenprodukt geschrieben

$$\begin{aligned} P(x)-e^{2\pi i/n} &= \left(x+\frac{1+\sqrt{1+4e^{2\pi i/n}}}{2}\right)\left(x+\frac{1-\sqrt{1+4e^{2\pi i/n}}}{2}\right) \\ &= g(x)h(x) = (x+A)(x+B)\,. \end{aligned}$$

Nämlich

$$\arg(1+ke^{2\pi i/n}) < \frac{2\pi}{n}$$

ist, wenn k eine große positive Zahl ist $\approx 2\pi/n$, und daher

$$\arg(1+4e^{2\pi i/n}) < \frac{2\pi}{n}\,,$$

infolge dessen ist

$$\arg\sqrt{1+4e^{2\pi i/n}} < \frac{2\pi}{2n} \quad \text{und} \quad \arg\frac{1+\sqrt{1+4e^{2\pi i/n}}}{2} < \frac{2\pi}{2n}\,,$$

also ist (s. den ersten Hilfssatz)

$$\arg\frac{1+\sqrt{1+4e^{2\pi i/n}}}{2} = \frac{2\pi}{4n}\,.$$

Es ist

$$A\cdot B = e^{2\pi i/n}, \qquad A\cdot B = 1\,,$$

A und B sind Einheiten aus dem Kreisteilungskörper K_n. Weiter ist erstens

$$\frac{1+\sqrt{1+4e^{2\pi i/n}}}{2} = \varepsilon_1\eta_1 = \varepsilon_1 e^{2\pi i/4n} = A$$

und zweitens

$$\frac{1-\sqrt{1+4e^{2\pi i/n}}}{2} = B = 1-A = 1-\varepsilon_1 e^{2\pi i/4n},$$

$$x^2-x-e^{2\pi i/n} = g(x)h(x) = (x+\varepsilon_1 e^{2\pi i/4n})(x+1-\varepsilon_1 e^{2\pi i/4n})\,.$$

Der Vergleich der Konstanten Glieder auf beiden Seiten ergibt

$$\varepsilon_1^2 e^{2\pi i/2n} - \varepsilon_1 e^{2\pi i/4n} - e^{2\pi i/n} = 0\,,$$

d.h.

$$\varepsilon_1^2 - \varepsilon_1 e^{-2\pi i/4n} - e^{2\pi i/2n} = 0\,,$$

woraus

$$\varepsilon_1 = \frac{e^{-2\pi i/4n} \pm \sqrt{e^{-2\pi i/2n}+4e^{2\pi i/2n}}}{2},$$

ε_1 ist eine reelle Zahl!

Das ist nur dann möglich, wenn $e^{-2\pi i/4n}$ konjugiert komplex zu $\pm\sqrt{e^{-2\pi i/2n}+4e^{2\pi i/2n}}$, d.h.

$$e^{2\pi i/4} = \pm\sqrt{e^{-2\pi i/2n}+4e^{2\pi i/2n}}.$$

Nach Quadrierung dieser Gleichung bekommen wir

$$e^{2\pi i/2n} - e^{-2\pi i/2n} = 4e^{2\pi i/2n},$$

d.h.

$$i\sin(2\pi/4n) = 2e^{2\pi i/2n}\,.$$

Die rechte Seite wird nur dann rein imaginär, wenn $n=2$, dann ist $i\sin(2\pi/8) = 2i$, was nicht sein kann.

Der Falle $m=1$ ist belanglos, da mit $F_n(x)$ auch das Polynom $F_n(x-a_1)$ über dem rationalen Körper irreduzibel ist (unter der Annahme, daß a_1 eine beliebig gewählte ganze rationale Zahl ist).

Damit ist der Beweis des Satzes V. vollendet.

Beweis des Satzes II. Nehmen wir an, daß das Polynom $-e^{2\pi i/n}+Q(x)\prod_{k=1}^{m}(x-a_k)$ über K_r reduzibel sei, d.h.

$$T(x)=Q(x)\prod_{k=1}^{m}(x-a_k)-e^{2\pi i/n}=g(x)h(x)\,,$$

wo das Polynom $g(x)$ von möglichst kleinstem Grade ($\geqslant 1$) ist. Es sei der höchste Koeffizient von $g(x)$ gleich Eins.

Auch die Zahlen $g(a_k)$ sind Einheiten aus dem Kreisteilungskörper K_r.

$$g(a_k)=\eta_k\varepsilon_k\,,\qquad g(a_l)=\eta_l\varepsilon_l\,,$$

wo η_k und η_l Einheitswurzeln, und ε_k und ε_l reelle Einheiten aus dem Körper K_r sind.

Wir haben

$$(a_k-a_l)/\big(g(a_k)-g(a_l)\big)\,,\qquad (a_k-a_l)/(\eta_k\varepsilon_k-\eta_l\varepsilon_l)\,.$$

Nach einer einfachen Umordnung erhalten wir

$$(a_k-a_l)/(\eta_k\eta_l^{-1}-\varepsilon_l\varepsilon_k^{-1}) \tag{33}$$

und nach dem Übergang zu dem konjugiert komplexen Werte

$$(a_k-a_l)/(\eta_k^{-1}\eta_l-\varepsilon_l\varepsilon_k^{-1})\,. \tag{34}$$

Nach Subtraktion von (33) und (34) entsteht die Beziehung

$$|a_k-a_l|/|\eta_k\eta_l^{-1}-\eta_k^{-1}\eta_l|$$

der für alle Konjugierten von $\eta_k\eta_l^{-1}-\eta_k^{-1}\eta_l$ bezüglich dem Körper K_0 gültig ist.

Zu den Normen übergehend können wir schreiben

$$|N_r(a_k-a_l)|/|N_r(\eta_k\eta_l^{-1}-\eta_k^{-1}\eta_l)$$

(über dem Körper K_r).

Ist $|a_k-a_l|\geqslant 3$, so gelangen wir zu einem Widerspruch, da

$$\Big|\prod_{s}(\eta_k\eta_l^{-1}-\eta_k^{-1}\eta_l)^{(s)}\Big|\leqslant N_r(2)\,,$$

(wo das Produkt über sämtlichen Konjugierten von $\eta_k\eta_l^{-1}-\eta_k^{-1}\eta_l$ erstreckt ist).

Wir bekommen nur dann keinen Widerspruch, wenn

$$\eta_1=\pm\eta_2=\pm\eta_3=\ldots=\pm\eta_m$$

und $m\geqslant 6$ ist.

Sonst führen die Hilfssätze IV. und V. (unter Berücksichtigung der Tatsache, daß die Lagrange'sche Interpolationsformel für $g(x)$ ein reelles Polynom ergibt, zu einem Widerspruch).

Der Beweis des Satzes III. Nehmen wir an, daß das Polynom

$$T(x)=\prod_{k=1}^{m}(x-a_k)Q(x)-e^{2\pi t/n}$$

über dem Körper K_r reduzibel ist. Dann wird das Polynom $T(x)$ über den rn-ten Kreisteilungskörper K_{rn} (umso mehr) reduzibel. Der Körper K_{rn} enthält den Körper K_r und nach dem Satze II. ist das unmöglich.

Literaturverzeichnis

[1] A. Brauer – R. Brauer und H. Hopf, *Über Irreduzibilität einiger speziellen Klasse von Polynomen*, Jahresbericht d. Deutschen Math. Ver.

[2] H. L. Dorwart – Oystein Ore, *Criteria for irreducibility of polynomials*, Ann. Math. 34 (1933), S. 81-94.

[3] W. Flügel, *Lösung der Aufgabe 226*, Archiv Math. Phys. 15 (1909), S. 271-272.

[4] L. Kronecker's Werke, *Über komplexe Einheiten*, Berlin 1895, S. 109-118.

[5] G. Pólya – G. Szegö, *Aufgaben und Lehrsätze der Analysis II*, Berlin 1925.

[6] I. Schur, *Aufgabe 226*, Archiv Math. Phys. 13 (1908), S. 367.

[7] — *Aufgabe 275*, Archiv Math. Phys. 15 (1909), S. 259.

[8] I. Seres, *Lösung und Verallgemeinerung eines Schur'schen Irreduzibilitätsproblems für Polynome*, Acta Math. Acad. Sci. Hungaricae, Budapest 1956, S. 151-157.

[9] — *Bizonyos polinomok irreducibilitása a körosztási testben*, A Magyar Tudományos Akadémia III. Osztályának Közleményei, Budapest 1960. X. kötet, S. 341-351. oldal.

[10] N. Tschebotarëw – H. Schwerdtfeger, *Grundzüge der Galois'schen Theorie*, Gröningen-Djakarta 1950, S. 288.

Reçu par la Rédaction le 15. 1. 1963