Ueber die Zerlegbarkeit der Function $x^n - a$ in einem beliebigen Körper.

Von

E. WENDT in Elsfleth a. d. Weser.

Im 2. Hefte des 19. Bandes der „Acta mathematica“ hat Herr Vahlen folgenden Satz bewiesen: „Alle im Bereiche der rationalen Zahlen reduciblen Binome erhält man aus den beiden

$$x^m - 1 \quad \text{und} \quad x^4 + 4$$

durch die Substitution $x \parallel \frac{z^n}{c}$, wo c eine rationale Zahl ist“.

Im Folgenden will ich den Ausdruck $x^n - a$ auf seine Zerlegbarkeit hin unter Zugrundelegung eines beliebigen Rationalitätsbereichs untersuchen.

1.

Es sei ξ eine Wurzel der Gleichung

$$(1) \quad \xi^n - a = 0$$

und ε eine primitive Wurzel der Gleichung

$$\varepsilon^n = 1.$$

Der zu Grunde gelegte Körper, dem a natürlich angehören muss, heisse K . Die übrigen Wurzeln der Gleichung (1) haben die Gestalt

$$\xi\varepsilon, \xi\varepsilon^2, \dots, \xi\varepsilon^{n-1}.$$

Der irreducible Factor von $x^n - a$, der für $x = \xi\varepsilon$ verschwindet, sei

$$(2) \quad f(x) = (x - \xi\varepsilon^{k_1})(x - \xi\varepsilon^{k_2}) \dots (x - \xi\varepsilon^{k_\varrho}); \quad (k_1 = 1); \quad (\varrho < n).$$

Das von x freie Glied dieses Productes muss eine in K rationale Zahl sein, also

$$(3) \quad \xi^\varrho \cdot \varepsilon^{k_1 + k_2 + \dots + k_\varrho} = \xi^\varrho \cdot \varepsilon^{\sum k} = a_\varrho.$$

Bezeichnet man dann den grössten gemeinsamen Theiler von ϱ und n mit d , setzt also

$$\varrho = d\varrho_1; \quad n = dn_1; \quad (n_1 > 1)$$

wobei ϱ_1 und n_1 theilerfremd sind, so lassen sich zwei ganze rationale Zahlen ϱ' und n' finden, derart, dass die Gleichung besteht

$$\varrho\varrho' + nn' = d.$$

Erhebt man die Seiten der Gleichung (3) auf die ϱ'^{te} Potenz, die der Gleichung (1) auf die n'^{te} Potenz und multiplicirt dann die entstehenden Gleichungen, so ergibt sich

$$(4) \quad \xi^d \cdot \varepsilon^{\varrho' \Sigma k} = a^{n'} \cdot a_{\varrho}^{\varrho'} = b,$$

wo b rational in K ist, und durch Erheben auf die n_1^{te} Potenz

$$(5) \quad a \cdot \varepsilon^{n_1 \varrho' \Sigma k} = b^{n_1}.$$

Nunmehr bilde man die Coefficienten der Glieder $x^{\varrho-\sigma}$ und x^{σ} der Function $f(x)$. Dann hat man

$$(6) \quad \xi^{\sigma} L_{\sigma} = a_{\sigma}; \quad \xi^{\varrho-\sigma} \varepsilon^{\Sigma k} L'_{\sigma} = a_{\varrho-\sigma} \quad (\sigma = 1, 2, \dots, \varrho-1),$$

wobei a_{σ} und $a_{\varrho-\sigma}$ rational in K sind, ferner

$$(6a) \quad L_{\sigma} = \varepsilon^{l_{1,\sigma}} + \varepsilon^{l_{2,\sigma}} + \dots; \quad L'_{\sigma} = \varepsilon^{-l_{1,\sigma}} + \varepsilon^{-l_{2,\sigma}} + \dots$$

ist und $l_{1,\sigma}; l_{2,\sigma}; \dots$ alle möglichen Summen von je σ verschiedenen Zahlen $k_1, k_2, \dots, k_{\varrho}$ bedeuten.

Unter den Grössen $a_{\sigma} (\sigma = 1, 2, \dots, \varrho-1)$ seien

$$a_{\sigma_1}, a_{\sigma_2}, \dots$$

die von Null verschiedenen; dann verschwinden also auch nicht die rationalen Functionen $L_{\sigma_1}, L_{\sigma_2}, \dots$ von ε . Den grössten gemeinschaftlichen Theiler der Zahlen $\sigma_1, \sigma_2, \dots$ und der Zahl d kann man für die weitere Untersuchung gleich 1 annehmen. Denn wird derselbe mit δ bezeichnet, so hat der irreducible Factor $f(x)$ von $x^n - a$ die Gestalt

$$x^{\varrho} + a_{\delta} x^{\varrho-\delta} + a_{2\delta} x^{\varrho-2\delta} + \dots + a_{\varrho-\delta} x^{\delta} + a_{\varrho},$$

ist also eine blosser Function von x^{δ} ; mithin muss $x^{\frac{n}{\delta}} - a$ den irreduciblen Factor

$$x^{\frac{\varrho}{\delta}} + a_{\delta} x^{\frac{\varrho}{\delta}-1} + a_{2\delta} x^{\frac{\varrho}{\delta}-2} + \dots + a_{\varrho-\delta} x + a_{\varrho}$$

besitzen. Unter der die Allgemeinheit nicht beschränkenden Annahme $\delta = 1$ lassen sich ganze rationale Zahlen $\sigma_1', \sigma_2', \dots, d'$ finden, derart dass

$$\sigma_1 \sigma_1' + \sigma_2 \sigma_2' + \dots + d d' = 1$$

ist. Aus den Gleichungen (4), (5) und (6) ergibt sich zunächst

$$\xi^{\sigma_1} = a_{\sigma_1} \cdot L_{\sigma_1}^{-1}; \quad \xi^{\sigma_2} = a_{\sigma_2} \cdot L_{\sigma_2}^{-1}; \dots; \xi^d = b \varepsilon^{-\varrho' \Sigma k}.$$

Durch Erheben der Seiten dieser Gleichungen bzw. auf die $\sigma_1'^{\text{te}}, \sigma_2'^{\text{te}}, \dots, d'^{\text{te}}$ Potenz und Multiplication der dadurch entstehenden Gleichungen folgt:

$$\xi = a_{\sigma_1}^{\sigma_1'} \cdot a_{\sigma_2}^{\sigma_2'} \dots b^{d'} \cdot L_{\sigma_1}^{-\sigma_1'} \cdot L_{\sigma_2}^{-\sigma_2'} \dots \varepsilon^{-\varrho' d' \Sigma k},$$

also

$$(7) \quad \xi = A \cdot g(\varepsilon)$$

und

$$(8) \quad a = \xi^n = A^n \cdot g(\varepsilon)^n,$$

wobei A rational in K ist und

$$(9) \quad g(\varepsilon) = L_{\sigma_1}^{-\sigma_1'} \cdot L_{\sigma_2}^{-\sigma_2'} \cdot \dots \cdot \varepsilon^{-\sigma' \cdot \Sigma k}$$

eine rationale Function von ε darstellt, deren Coefficienten dem natürlichen Bereiche, der mit P bezeichnet werden möge, angehören.

Wenn also $x^n - a$ reducibel sein soll, muss a dargestellt werden können als ein Product der n^{ten} Potenz einer in K rationalen Zahl und der n^{ten} Potenz einer rationalen Function von ε , deren Coefficienten in P rational sind. Umgekehrt, wenn diese Darstellung möglich ist, so gilt eine Gleichung von der Form der Gleichung (7), und da ε im Körper P einer Gleichung genügt, deren Grad nur $\varphi(n)$ ist, so sind auch $g(\varepsilon)$ und damit ξ in K Wurzeln einer Gleichung vom Grade $\varphi(n)$, also ist der Ausdruck $x^n - a$ reducibel. Somit ist folgender Satz bewiesen.

Ein Ausdruck von der Form $x^m - a$ ist dann und nur dann reducibel in einem Körper K , wenn sich a als Product der n^{ten} Potenz einer in K rationalen Zahl und der n^{ten} Potenz einer rationalen Function von ε , deren Coefficienten dem natürlichen Bereiche entstammen, darstellen lässt, wobei n ein Theiler von m ist und ε eine primitive n^{te} Einheitswurzel bedeutet.

2.

Diesem Resultat will ich zunächst für den Fall eine andere Form geben, dass in K keine wirkliche ganze rationale Function von ε , deren Coefficienten dem natürlichen Bereiche P angehören, rational ist.

Durch Multiplication der Gleichungen unter (6) ergibt sich mit Hülfe von (3)

$$(10) \quad L_\sigma L'_\sigma = \frac{a_\sigma a_{q-\sigma}}{a_q} = B_\sigma,$$

wo B_σ eine in K rationale Zahl bedeutet. Zufolge der Gleichung (8) gehört $g(\varepsilon)^n$ zum Bereiche K ; diese Grösse muss daher gemäss der über den Körper gemachten Voraussetzung eine natürliche Zahl sein. Bezeichnet man sie mit C und erwägt, dass L'_σ aus L_σ entsteht, wenn man $+i$ durch $-i$ ersetzt, so folgt mit Hülfe der Gleichung (9):

$$[(L_{\sigma_1} \cdot L'_{\sigma_1})^{-\sigma_1'} \cdot (L_{\sigma_2} \cdot L'_{\sigma_2})^{-\sigma_2'} \cdot \dots]^n = C^2,$$

also nach (10)

$$(B_{\sigma_1}^{-\sigma_1'} \cdot B_{\sigma_2}^{-\sigma_2'} \cdot \dots)^n = C^2,$$

oder

$$C^2 = B^n,$$

wo B eine in K rationale Zahl bedeutet.

Ist n ungerade, so würde folgen, dass C und somit auch a die n^{te} Potenz einer in K rationalen Zahl wäre, und dann ist $x^n - a$ sicher reducibel. Ist n gerade, so ergibt sich

$$C = \pm B^{\frac{n}{2}} \quad \text{und} \quad a = \pm (A^2 \cdot B)^{\frac{n}{2}} = \pm D^{\frac{n}{2}},$$

wo D rational in K ist. Enthält n irgend eine ungerade Zahl als Divisor oder gilt das positive Zeichen, so ist $x^n - a$ thatsächlich reducibel. Es erübrigt daher nur noch den Fall

$$a = -D^{\frac{n}{2}}; \quad n = 2^v,$$

also die Function

$$x^n + D^{\frac{n}{2}} = x^{2^v} + D^{2^{v-1}}$$

zu betrachten.

Aus der Gleichung $\xi^n = -D^{\frac{n}{2}}$ folgt zunächst $\xi^2 = D \cdot \eta$, wo η eine primitive n^{te} Einheitswurzel bedeutet. Man kann sich nun ξ so gewählt denken, dass $\eta = \varepsilon$ ist, also

$$(11) \quad \xi^2 = D \cdot \varepsilon.$$

Hierzu kommen noch die Gleichungen:

$$(12) \quad \xi(\varepsilon^{k_1} + \varepsilon^{k_2} + \dots + \varepsilon^{k_\varphi}) = a_1; \quad \xi^2(\varepsilon^{1,2} + \varepsilon^{2,2} + \dots) = a_2.$$

Durch Quadriren der beiden Seiten der ersteren dieser Gleichungen erhält man mit Benutzung der letzteren und der Gleichung (11)

$$(13) \quad \varepsilon(\varepsilon^{2k_1} + \varepsilon^{2k_2} + \dots + \varepsilon^{2k_\varphi}) = \frac{a_1^2 - 2a_2}{D}.$$

Da aber im vorliegenden Falle ε eine Wurzel der irreduciblen Gleichung $\varepsilon^{\frac{n}{2}} + 1 = 0$ und $\varphi \geq 2$ ist, so kann diese Gleichung infolge der dem Körper K auferlegten Einschränkung nur bestehen, falls $a_1^2 = 2a_2$ ist. Ferner folgt aus der zweiten der Gleichungen (12)

$$(14) \quad \varepsilon(\varepsilon^{1,2} + \varepsilon^{2,2} + \dots) = \frac{a_2}{D}.$$

Für $\varphi > 2$ kann diese Gleichung, weil dann die Klammer eine gerade Anzahl von Gliedern enthält, nur bestehen, wenn a_2 und somit a_1 verschwindet, und zu dem Ende muss der Ausdruck $L_1 = \varepsilon^{k_1} + \dots + \varepsilon^{k_\varphi}$ gleich Null sein, folglich muss sich die Function $f(x)$, da die Glieder von L_1 wegen der Irreducibilität der Gleichung $\varepsilon^{\frac{n}{2}} + 1 = 0$ paarweise verschwinden müssen, als ein Product von der Form

$$\prod_{\sigma=1}^{\frac{\varrho}{2}} (x + \varepsilon^{k_{\sigma}} \xi) (x - \varepsilon^{k_{\sigma}} \xi) = \prod_{\sigma=1}^{\frac{\varrho}{2}} (x^2 - \varepsilon^{2k_{\sigma}} \xi^2)$$

darstellen, wäre also eine blosser Function von x^2 , die $f_1(x^2)$ heisse. Wenn aber $x^n + D^{\frac{n}{2}}$ den irreduciblen Factor $f(x) = f_1(x^2)$ besitzen soll, muss $x^{\frac{n}{2}} + D^{\frac{n}{4}}$, ($n = 2^{\nu}$) durch $f_1(x)$ theilbar sein. Da aber $x^{\frac{n}{2}} + D^{\frac{n}{4}}$ irreducibel ist, so folgt rückwärts, dass $\varrho = 2$ sein muss. Dann aber lautet Gleichung (14)

$$\varepsilon \cdot \varepsilon^{k_1+k_2} = \frac{a_2}{D},$$

und da ausserdem $k_1 = 1$ und $\varepsilon^{2k_1} + \varepsilon^{2k_2} = 0$, also $2k_2 = \frac{n}{2} + 2$ ist,

so folgt $\varepsilon^{\frac{n}{4}+2} = \frac{a_2}{D} = \pm 1$, also $D = \pm a_2 = \pm \frac{a_1^2}{2}$ und $n = 4$. Setzt man demnach $a_1 = 2y$, so erhält man die Gleichung

$$(15) \quad x^4 + 4y^4 = (x^2 - 2yx + 2y^2) \cdot (x^2 + 2yx + 2y^2).$$

Demzufolge gilt der Satz:

Die Function $x^n - a$ ist in einem Körper K , dem keine wirkliche ganze rationale Function von ε mit natürlichen Zahlen-coefficienten angehört, nur in folgenden beiden Fällen reducibel:

1) *wenn a die r^{te} Potenz einer in K enthaltenen Zahl ist, wo r in n aufgeht;*

2) *wenn n und a die Form haben $n = 4\delta$, $a = 4y^4$, wo δ eine ganze rationale Zahl bedeutet und y rational in K ist; und zwar sind die beiden Factoren der Function*

$$x^{4\delta} + 4y^4 = (x^{2\delta} - 2yx^{\delta} + 2y^2) (x^{2\delta} + 2yx^{\delta} + 2y^2)$$

irreducibel in K .

Die Richtigkeit der letzten Behauptung ergibt sich folgendermassen. Angenommen, der eine der Factoren wäre reducibel, er hätte den irreduciblen Factor $f(x) = x^{\varrho} + a_1 x^{\varrho-1} + \dots + a_{\varrho-1} x + a_{\varrho}$, dann kann man annehmen, dass der grösste gemeinschaftliche Divisor der Indices $1, 2, 3, \dots, \varrho$ der nichtverschwindenden Coefficienten gleich 1 sei (denn andernfalls würde folgen, dass ein Ausdruck von der Form $x^{2\delta'} + 2yx^{\delta'} + 2y^2$, wo δ' ein Theiler von δ bedeutet, reducibel wäre, und dann würde man diesen zu untersuchen haben), und die in den Absätzen 1) und 2) befolgte Schlussweise kann angewendet werden. Diese führt, da $n = 4\delta$ gerade ist,

entweder zu der Forderung $a = -D^{\frac{n}{2}}$, d. h. $-4y^4 = -D^{2\delta}$ oder zu der Forderung $\varrho = 2$, in jedem Falle also müsste $n = 4$ sein, d. h. es müsste $x^2 + 2xy + 2y^2$ reducibel sein, und das ist nicht der Fall.

3.

Ich wende mich nun dem Falle zu, wo wirkliche rationale Functionen von ε mit natürlichen Zahlencoefficienten Grössen des Bereichs sind.

Wird zunächst der Fall in's Auge gefasst, dass keine imaginäre n^{te} Einheitswurzel selbst zum Bereiche gehört, so fordert die Gleichung (5), dass

$$\varepsilon^{n_1 \rho' \Sigma k} = \pm 1, \quad \text{also} \quad a = \pm b^n$$

ist. Gilt das positive Zeichen oder enthält n_1 eine ungerade Zahl als Factor, so ist $x^n - a$ thatsächlich reducibel. Andernfalls muss $n_1 \rho' \Sigma k$ ein Vielfaches von $\frac{n}{2}$, aber nicht von n sein, d. h. d muss gerade und daher n durch 4 theilbar sein.

Bis zu demselben Punkte will ich nun zunächst die Untersuchung für den Fall führen, dass eine imaginäre n^{te} Einheitswurzel zum Bereiche gehört. Es sei $\eta = \varepsilon^t$ die niedrigste Potenz von ε , welche in K rational ist; t muss dann ein Divisor von n sein.

Es wäre nun möglich, dass die irreducible Gleichung $f(x) = 0$, welcher ξ genügt, auch durch einen Werth $\xi \cdot \xi$ befriedigt wird, wo ξ eine in K rationale n^{te} Einheitswurzel bedeutet. Wenn aber $f(\xi \cdot \xi) = 0$ ist, so muss wegen der Irreducibilität von $f(x)$ auch $f(\xi \cdot \xi^2) = 0$; $f(\xi \cdot \xi^3) = 0$; $\dots$; $f(\xi \cdot \xi^{\tau-1}) = 0$ sein, wo $\xi^\tau = 1$ sei. Ist ferner ξ_1 eine von den bisher erwähnten Wurzeln verschiedene, so müssen auch $\xi_1 \cdot \xi$; $\xi_1 \cdot \xi^2$; $\dots$; $\xi_1 \cdot \xi^{\tau-1}$ Wurzeln sein. Folglich enthält $f(x)$ lauter Factoren von der Form

$$(x - \xi) (x - \xi \xi) (x - \xi \xi^2) \dots (x - \xi \xi^{\tau-1}) = x^\tau - \xi^\tau,$$

ist also eine blossе Function von x^τ , welche $f'(x^\tau)$ heisse. Wenn demnach $x^n - a$ den irreduciblen Factor $f(x) = f'(x^\tau)$ enthält, so muss $x^\tau - a$ den irreduciblen Factor $f'(x)$ enthalten. Daher kann man, ohne dass die Untersuchung an Allgemeinheit verliert, $\tau = 1$ annehmen.

Dieselbe Ueberlegung kann man in Bezug auf alle irreduciblen Factoren $f(x)$ anstellen. Man wird auf diese Weise zu einer Function $x^n - a$ geführt, von der kein irreducibler Factor für zwei durch einander rational ausdrückbare Grössen verschwindet. Es ist dann möglich, dass überhaupt keine zwei Wurzeln der Gleichung $\xi^n - a = 0$ rational von einander abhängig sind. Dann kommt man zu dem in diesem Absatz zuerst behandelten Falle zurück.

Andernfalls zerlegt sich $x^n - a$ in t' Factoren von der Form

$$\begin{aligned} f(x) &= (x - \xi \varepsilon^{k_1}) (x - \xi \varepsilon^{k_2}) \dots, \\ f_1(x) &= (x - \xi \varepsilon^{k_1} \eta) (x - \xi \varepsilon^{k_2} \eta) \dots, \\ &\vdots \\ f_{i-1}(x) &= (x - \xi \varepsilon^{k_1} \eta^{i'-1}) (x - \xi \varepsilon^{k_2} \eta^{i'-1}) \dots, \end{aligned}$$

wo jeder Factor aus t Linearfactoren besteht und wo $t \cdot t' = n$ und $\eta = \varepsilon^t$ wieder die niedrigste in K enthaltene Potenz von ε bedeute. Es folgt $\xi^t \cdot \varepsilon^{k_1 + k_2 + \dots} = \alpha$, wo α in K rational ist. Die Zahlen $k_1, k_2, \dots$ stimmen, von der Reihenfolge abgesehen, modulo t mit den Zahlen $0, 1, 2, \dots, t-1$ überein, daher ist ihre Summe $\equiv \frac{t}{2}$, resp. $0 \pmod{t}$, je nachdem t gerade oder ungerade ist. Durch Erheben der Seiten obiger Gleichung auf die t'^{te} Potenz ergibt sich infolgedessen

$$\pm a = \alpha^{t'}.$$

In weitere Erörterung ist also auch hier bloss noch der Fall zu ziehen, dass t' eine Potenz von 2 ist und dass das Minuszeichen gilt, dass also auch t gerade und n durch 4 theilbar ist.

Gehört $i = \varepsilon^{\frac{n}{4}}$ zum Bereiche K , so ist $x^n - a$, falls a die Form $-b^s$ hat, reducibel, weil dann $a = \left(b^{\frac{s}{2}} \cdot i\right)^2$ ist. Gehört aber i nicht zum Bereiche, so muss ε^{-1} Wurzel derselben in K irreduciblen Gleichung sein, welcher ε genügt, weil $(\varepsilon, \varepsilon^{-1})$ die einzige Transposition unter den primitiven n^{ten} Einheitswurzeln ist, welche $i = \varepsilon^{\frac{n}{4}}$ nicht unverändert lässt.

Nach dem im Abschnitt 1. bewiesenen Hauptsatze muss a , falls $x^n - a$ reducibel sein soll, in die Form $A^n g(\varepsilon)^n$ gebracht werden können. Es genügt also $g(\varepsilon)$ einer Gleichung $g(\varepsilon)^n = C$, wo C in K rational ist. Da ε^{-1} Wurzel derselben irreduciblen Gleichung ist, welcher ε genügt, so folgt $g(\varepsilon^{-1})^n = C$. Und sonach lässt sich wie im Abschnitt 2. weiter schliessen, dass a die Form $\pm D^{\frac{n}{2}}$ haben muss. Da die Function $x^n \mp D^{\frac{n}{2}}$ in K reducibel ist, welchen Werth auch n haben möge, weil eine rationale Function von ε zum Bereiche gehört, so ist folgender Satz bewiesen:

In einem Körper K , zu welchem eine rationale Function von ε mit natürlichen Zahlencoefficienten gehört, in dem also ε einer Gleichung von niederem als dem $\varphi(n)^{\text{ten}}$ Grade genügt, ist die Function $x^n - a$ nur in folgenden beiden Fällen reducibel:

1) wenn a die s^{te} Potenz einer in K rationalen Zahl ist, wo s ein Theiler von n ist;

2) wenn $n = 2^v$ und $a = -D^{\frac{n}{2}}$ ist, wo D dem Bereiche K angehört.