ÜBER REDUCTIBLE BINOME

VON

K. TH. VAHLEN

in BERLIN.

ABEL beweist in § II der *Démonstration de l'impossibilité de la résolution des équations générales qui passent le quatrième degré* den Satz:

Wenn n eine Primzahl ist, so kann eine n^{te} Wurzel einer rationalen Funktion beliebig vieler unabhängiger Variablen $x', x'', \ldots$ keiner Gleichung niederen als n^{ten} Grades genügen, deren Coëfficienten rationale Funktionen von $x', x'', \ldots$ sind.

Wir stellen uns allgemeiner die Aufgabe:

Wann kann eine n^{te} Wurzel einer dem natürlichen Rationalitätsbereich $(x', x'', \ldots)$ entstammenden rationalen Grösse einer Gleichung niederen als n^{ten} Grades genügen, deren Coëfficienten demselben Bereich angehören?

Der Rationalitätsbereich sei zunächst der der rationalen Zahlen. Ist c eine rationale Zahl und genügt $z = \sqrt[n]{c}$ einer Gleichung niedrigeren als n^{ten} Grades, welche mit der Gleichung $z^n - c = 0$ den irreductibeln Faktor $a + a_1 z + a_2 z^2 + \ldots + a_{m-1} z^{m-1} + z^m$ gemein hat, so zerfällt das Binom: $z^n - c$ in das Produkt:

$$(a + a_1 z + \ldots + z^m)(b + b_1 z + \ldots + z^{n-m}).$$

Durch Multiplikation des Binoms mit einem geeigneten Faktor und Einführung einer anderen Variablen z können wir bewirken, dass c eine ganze Zahl wird. Alsdann sind, nach einem bekannten Satze von GAUSS,[1] auch die Coëfficienten $a, a_1, \ldots, b, b_1, \ldots$ ganze Zahlen.

[1] Disquisitiones arithmeticae, art. 42.

Acta mathematica. 19. Imprimé le 21 mars 1895.

Ist jetzt wenigstens ein Wert von $\sqrt[n]{c}$ reell, so hat das Produkt der m Wurzeln der Gleichung:

$$a + a_1 z + \ldots + z^m = 0$$

absolut genommen einerseits den Wert $|a|$, andrerseits den Wert $|\sqrt[n]{c^m}|$. Aus der Gleichung:

$$|\sqrt[n]{c^m}| = |a|$$

folgt, dass c die ν^{te} Potenz einer positiven oder negativen ganzen Zahl, ν ein Teiler von n ist. Wir erhalten also das Binom: $z^{\mu\nu} - \gamma^\nu$.

Ist zweitens kein Wert von $\sqrt[n]{c}$ reell, d. h. ist n gerade, c negativ, so haben wir es mit dem Binom $z^{2n} + c$ zu thun, wo jetzt c eine positive ganze Zahl ist.

Ist $f(z)$ ein irreductibler Faktor von $z^{2n} + c$, so muss derselbe bei der Substitution

$$z \parallel -z$$

entweder in sich selbst oder in einen andern irreductibeln Faktor von $z^{2n} + c$ übergehen. Im ersten Fall wäre $f(z)$, also auch der complementäre Faktor $\frac{z^{2n} + c}{f(z)}$ eine ganze Function von z^2 und man erhielte durch die Substitution $z^2 \parallel z$ ein reductibles Binom halb so hohen Grades. Von derartig abgeleiteten Binomen können wir natürlich absehen.

Im zweiten Fall ist $f(z).f(-z)$ eine ganze Funktion von z^2; wir kommen also nur dann nicht auf den ersten Fall zurück, wenn $f(z)$ vom höchsten also n^{ten} Grade ist. Es kommt also nur die Zerlegung

$$(a + a_1 z + a^2 z^2 + \ldots + a_{n-1} z^{n-1} + z^n)(a - a_1 z + a_2 z^2 - \ldots + (-1)^{n-1} a_{n-1} z^{n-1} + (-1)^n z^n)$$

in Betracht, die aber für ungrades n auf das Binom $a^2 - z^{2n}$ führt. Es muss also n gerade sein, und daher ist nur noch die Zerlegung:

$$z^{4n} + a^2 = (a + a_1 z + \ldots + z^{2n})(a - a_1 z + \ldots + z^{2n})$$

zu untersuchen.

Die Coëfficienten a genügen den Gleichungen:

$$\begin{aligned} 2aa_2 - a_1^2 &= 0, \\ 2aa_4 - 2a_1a_3 + a_2^2 &= 0, \\ 2aa_6 - 2a_1a_5 + 2a_2a_4 - a_3^2 &= 0, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \\ 2a - 2a_1a_{2n-1} + 2a_2a_{2n-2} - \ldots \pm a_n^2 &= 0. \end{aligned}$$

Ist p ein Primfaktor von $2a$, so folgt aus diesen Gleichungen der Reihe nach, dass auch $a_1, a_2, \ldots, a_n$ durch p teilbar sein müssen, und dann aus der letzten, dass $2a$ durch p^2 teilbar sein muss.

Setzt man

$$2a = p^2b, \qquad a_i = p \cdot b_i \qquad (i=1,2,\ldots,n)$$

so gestatten die Gleichungen:

$$\begin{aligned} pbb_2 - b_1^2 &= 0, \\ pbb_4 - 2b_1b_3 + b_2^2 &= 0, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \\ b - 2b_1b_{2n-1} + \ldots \pm b_n^2 &= 0 \end{aligned}$$

denselben Schluss in Bezug auf einen Primfaktor von b. Durch Fortsetzung dieses Verfahrens ergiebt sich, dass $2a$ ein Quadrat, also $a = 2c^2$ sein muss. Das Binom $z^{4n} + 4c^4$ ist aber durch die Substitution $z \left\| \frac{z^n}{c} \right.$ aus dem Binom:

$$z^4 + 4$$

abgeleitet, und dieses letztere ist in der That reductibel; es ist:

$$z^4 + 4 = (z^2 - 2z + 2)(z^2 + 2z + 2).$$

Zusammenfassend können wir den Satz aussprechen:

Alle im Bereich der rationalen Zahlen reductiblen Binome erhält man aus den beiden:

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

durch die Substitution $z \left\| \frac{z^n}{c} \right.$, *wo* c *eine rationale Zahl ist.*

Der Satz ist ohne Mühe auf den natürlichen Rationalitätsbereich beliebig vieler unabhängiger Variablen auszudehnen, und bedeutet alsdann c eine rationale Grösse dieses Bereiches.

Über das merkwürdige Binom

$$z^4 + 4,$$

das also, von trivialen Fällen abgesehen, das einzige reductible ist, finden sich in LUCAS, *Théorie des nombres,* interessante historische Notizen. So hatte schon SOPHIE GERMAIN den Satz ausgesprochen: Das Binom $z^4 + 4$ stellt ausser 5 keine Primzahl dar.

Für $z = 2^{-n}$ ergiebt sich die Zerlegung:

$$2^{4n+2} + 1 = (2^{2n+1} + 2^{n+1} + 1)(2^{2n+1} - 2^{n+1} + 1),$$

aus welcher z. B. für $n = 14$ die Zerlegung von $2^{58} + 1$ folgt, eine Zerlegung, die LANDRY lange vergeblich gesucht hat, und die ihm von allen in seiner *Décomposition des nombres* $2^n \pm 1$ *en leurs facteurs premiers, de* $n = 1$ *à* $n = 64$, *moins quatre* (Paris, 1869) ausgeführten Zerlegungen weitaus die grössten Schwierigkeiten gemacht hat.