DER FUNDAMENTALSATZ DER ALGEBRA UND DIE AUFLÖSUNG DER GLEICHUNGEN DURCH QUADRATWURZELN.

VON

K. TH. VAHLEN
in KÖNIGSBERG.

1. Es sei $f(x) = 0$ eine Gleichung n-ten Grades, deren n Wurzeln $x_1, \ldots, x_n$ von einander verschieden seien.

Man bilde die zwei Reihen von je $\left[\frac{n}{2}\right]$ Grössen:

$$\begin{array}{cccccccc} x_1 + x_2 \,, & x_3 + x_4 \,, & x_5 + x_6 \,, & x_7 + x_8 \,, & \ldots \\ x_1 x_2 \,, & x_3 x_4 \,, & x_5 x_6 \,, & x_7 x_8 \,, & \ldots; \end{array}$$

von den n Grössen $x_1, \ldots, x_n$ bleiben dabei $n - 2\left[\frac{n}{2}\right]$ Grössen — nämlich eine, x_n, oder keine — übrig.

Aus jeder der beiden Reihen bilde man ebenso zwei neue, so dass man vier Reihen von je $\left[\frac{n}{4}\right]$ Grössen erhält:

$$\begin{array}{ccc} x_1 + x_2 + x_3 + x_4 \,, & x_5 + x_6 + x_7 + x_8 \,, & \ldots \\ (x_1 + x_2)(x_3 + x_4) \,, & (x_5 + x_6)(x_7 + x_8) \,, & \ldots \\ x_1 x_2 + x_3 x_4 \,, & x_5 x_6 + x_7 x_8 \,, & \ldots \\ x_1 x_2 x_3 x_4 \,, & x_5 x_6 x_7 x_8 \,, & \ldots; \end{array}$$

dabei bleiben von jeder der obigen zwei Reihen

$$\left[\frac{n}{2}\right] - 2\left[\frac{\left[\frac{n}{2}\right]}{2}\right] = \left[\frac{n}{2}\right] - 2\left[\frac{n}{4}\right]$$

Grössen übrig.

Verfährt man mit den vier Reihen ebenso, so erhält man acht neue Reihen und in jeder der vier Reihen bleiben

$$\left[\frac{n}{4}\right] - 2\left[\frac{\left[\frac{n}{4}\right]}{2}\right] = \left[\frac{n}{4}\right] - 2\left[\frac{n}{8}\right]$$

Grössen übrig.

So fortfahrend, bis man keine neuen Reihen mehr bilden kann, erhält man im Ganzen:

$$n - 2\left[\frac{n}{2}\right] + 2\left[\frac{n}{2}\right] - 4\left[\frac{n}{4}\right] + 4\left[\frac{n}{4}\right] - 8\left[\frac{n}{8}\right] + \ldots = n$$

übrig bleibende Grössen, die in irgend einer Reihenfolge mit $x^{(1)}, \ldots, x^{(n)}$ bezeichnet werden mögen.

2. Wenn zwei zusammengehörige Werte für $x_1 + x_2$ und $x_1 x_2$ bekannt sind, so ist dadurch das Wurzelpaar x_1, x_2 bis auf die Reihenfolge eindeutig bestimmt. Denn, ist x_{i_1}, x_{i_2} ein anderes Wurzelpaar, also wenigstens einer der Indices i_1, i_2 von 1 und 2 verschieden, so würde aus:

$$x_1 + x_2 = x_{i_1} + x_{i_2}$$
$$x_1 x_2 = x_{i_1} x_{i_2}$$

die Übereinstimmung beider Wurzelpaare, also die Existenz wenigstens einer Doppelwurzel folgen; aber dies war ausgeschlossen. Die Grösse $u_1(x_1 + x_2) + u_2 x_1 x_2$, mit Unbestimmten u_1, u_2, nimmt also bei allen Permutationen der n Wurzeln $\frac{n(n-1)}{1 \cdot 2}$ verschiedene Werte an, welche einer Gleichung mit nicht identisch verschwindender Discriminante $D(u_1, u_2)$ genügen. Giebt man, was also möglich ist, den Unbestimmten u_1, u_2 solche rationalen Werte, dass $D(u_1, u_2) \neq 0$ ist, so sind nach einem bekannten Satze $x_1 + x_2$ und $x_1 x_2$ rationale Funktionen von $u_1(x_1 + x_2) + u_2 x_1 x_2$.

Sind nämlich, allgemeiner, g_1 und g_2 rationale Functionen der Wurzeln und genügt $z = u_1 g_1 + u_2 g_2$ mit Unbestimmten u_1, u_2 der irreductibeln Gleichung $F(z; u_1, u_2) = 0$, aber $z = v_1 g_1 + v_2 g_2$ mit Bestimmten v_1, v_2 der irreductibeln Gleichung $F_1(z) = 0$, so ergibt sich $z = v_1 g_1 + v_2 g_2$ als *einzige* gemeinsame Wurzel der beiden Gleichungen: $F_1(z) = 0$ und $F(z - u_1 g_1 - u_2 g_2; v_1 - u_1, v_2 - u_2) = 0$, also als rationale Funktion von $u_1 g_1 + u_2 g_2$. Denn eine andere Wurzel der zweiten Gleichung: $z = u_1 g_1 + u_2 g_2 + (v_1 - u_1) g_1' + (v_2 - u_2) g_2'$ könnte der ersten: $F_1(z) = 0$ bei beliebigen u_1, u_2 nur genügen, wenn $u_1 g_1 + u_2 g_2 = u_1 g_1' + u_2 g_2'$ ist, so dass $F(z; u_1, u_2)$ nicht irreductibel wäre.

3. Wenn vier zuzammengehörige Werte für

$$x_1 + x_2 + x_3 + x_4, \quad (x_1 + x_2)(x_3 + x_4), \quad x_1 x_2 + x_3 x_4, \quad x_1 x_2 x_3 x_4$$

bekannt sind, so ergeben sich $x_1 + x_2$ und $x_1 x_2$ als Wurzeln quadratischer Gleichungen, also zweideutig. Wie diese Werte zusammengehören ergiebt sich aus 2. Alsdann ergeben sich die Werte von x_1 und x_2, ebenso von x_3 und x_4 als Wurzeln quadratischer Gleichungen. Ist $x_{i_1}, x_{i_2}, x_{i_3}, x_{i_4}$ ein anderes Wurzelquadrupel, also wenigstens einer der Indices i_1, i_2, i_3, i_4 verschieden von 1, 2, 3, 4, so würde aus den Gleichungen:

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= x_{i_1} + x_{i_2} + x_{i_3} + x_{i_4} \\ (x_1 + x_2)(x_3 + x_4) &= (x_{i_1} + x_{i_2})(x_{i_3} + x_{i_4}) \\ x_1 x_2 + x_3 x_4 &= x_{i_1} x_{i_2} + x_{i_3} x_{i_4} \\ x_1 x_2 x_3 x_4 &= x_{i_1} x_{i_2} x_{i_3} x_{i_4} \end{aligned}$$

die Übereinstimmung beider Wurzelquadrupel — von der Reihenfolge abgesehen —, also die Existenz mindestens einer Doppelwurzel folgen; aber dies war ausgeschlossen. Die Grösse

$$u_1(x_1 + x_2 + x_3 + x_4) + u_2(x_1 + x_2)(x_3 + x_4) \\ + u_3(x_1 x_2 + x_3 x_4) + u_4 x_1 x_2 x_3 x_4,$$

mit Unbestimmten u_1, u_2, u_3, u_4, genügt daher einer Gleichung vom Grade $\frac{n(n-1)(n-2)(n-3)}{8}$ mit nicht identisch verschwindender Discriminante

$D(u_1, u_2, u_3, u_4)$. Giebt man, was also möglich ist, den Unbestimmten $u_1, u_2, u_3 . u_4$ solche rationalen Werte, dass $D(u_1, u_2, u_3, u_4) \neq 0$ ist, so sind

$$x_1 + x_2 + x_3 + x_4\,, \; (x_1 + x_2)(x_3 + x_4)\,, \; x_1 x_2 + x_3 x_4\,, \; x_1 x_2 x_3 x_4$$

rationale Funktionen von

$$u_1(x_1 + x_2 + x_3 + x_4) + u_2(x_1 + x_2)(x_3 + x_4) \\ + u_3(x_1 x_2 + x_3 x_4) + u_4 x_1 x_2 x_3 x_4 \,.$$

4. So fortfahrend erkennt man, dass sich die n Wurzeln $x_1, \ldots, x_n$ in bestimmter — d. h. bis auf die Reihenfolge bestimmter — Weise durch blosses Quadratwurzelausziehen ergeben, wenn die Werte der n Grössen $x^{(1)}, \ldots, x^{(n)}$ bekannt sind.

Bilden wir die Funktion $u = u^{(1)}x^{(1)} + \ldots + u^{(n)}x^{(n)}$, zunächst mit Unbestimmten $u^{(1)}, \ldots, u^{(n)}$. Die Funktion u bleibt ungeändert bei den $\left[\frac{n}{2}\right]$ Vertauschungen von x_1 mit x_2, von x_3 mit x_4, von x_5 mit x_6, von x_7 mit x_8, u. s. w., ferner bei den $\left[\frac{n}{4}\right]$ Vertauschungen von x_1, x_2 mit x_3, x_4, von x_5, x_6 mit x_7, x_8, u. s. w., ferner bei den $\left[\frac{n}{8}\right]$ Vertauschungen von x_1, x_2, x_3, x_4 mit x_5, x_6, x_7, x_8, u. s. w., u. s. w. Die Funktion u kann also nur bei $\dfrac{\underline{|n}}{2^{\left[\frac{n}{2}\right] + \left[\frac{n}{4}\right] + \left[\frac{n}{8}\right] + \cdots}} = N$ Permutationen der Wurzeln verschiedene Werte annehmen; die entsprechenden Werte sind wirklich, bei Unbestimmten $u^{(1)}, \ldots, u^{(n)}$, alle von einander verschieden. Denn sonst wäre etwa:

$$x^{(1)} = \bar{x}^{(1)}$$
$$\cdots\cdots$$
$$\cdots\cdots$$
$$x^{(n)} = \bar{x}^{(n)},$$

wo $\bar{x}^{(1)}, \ldots, \bar{x}^{(n)}$ die den $x^{(1)}, \ldots, x^{(n)}$ analogen Funktionen von den in anderer Reihenfolge genommenen Wurzeln $\bar{x}_1, \ldots, \bar{x}_n$ bedeuten, und sich diese

Reihenfolge von der ursprünglichen $x_1, \ldots, x_n$ nicht nur durch zulässige Vertauschungen unterscheidet. Daraus würde sich, bis auf zulässige Vertauschungen, die Übereinstimmung von $x_1, \ldots, x_n$ mit $\bar{x}_1, \ldots, \bar{x}_n$, also die Existenz wenigstens einer Doppelwurzel ergeben. Da dies ausgeschlossen war, genügt u einer Gleichung $G(u) = 0$ vom Grade N und von nicht identisch verschwindender Discriminante $D(u^{(1)}, \ldots, u^{(n)})$. Giebt man, was also möglich ist, den Grössen $u^{(1)}, \ldots, u^{(n)}$ solche rationalen Werte, dass $D(u^{(1)}, \ldots, u^{(n)}) \neq 0$ ist, so sind $x^{(1)}, \ldots, x^{(n)}$ rationale Funktionen von u, und die vollständige Auflösung der Gleichung $f(x) = 0$ durch Quadratwurzeln ist zurückgeführt auf die Auffindung einer Wurzel der Resolvente $G(u) = 0$.

5. Hat also $G(u) = 0$ eine rationale Wurzel, so sind sämmtliche Wurzeln von $f(x) = 0$ durch Quadratwurzeln darstellbar. Dasselbe findet aber auch umgekehrt statt. Es sei der Wert einer Wurzel x_1 durch α und nicht weniger Quadratwurzelausziehungen zu ermitteln; dann ist die allgemeinste Annahme die, dass der Radicand jeder später auszuziehenden Wurzel, aber nicht diese Wurzel selbst, von den bereits ausgezogenen Wurzeln rational abhängt. Die Gleichung $f(x_1) = 0$ nimmt in Bezug auf die letzte Quadratwurzel $\sqrt{r_\alpha}$ die Form an: $A + B\sqrt{r_\alpha} = 0$, wo A, B und r_α, aber nicht $\sqrt{r_\alpha}$ von den vorhergehenden Quadratwurzeln $\sqrt{r_1}, \sqrt{r_2}, \ldots, \sqrt{r_{\alpha-1}}$ rational abhängen; daraus folgt $A = 0$, $B = 0$, da $r_\alpha \neq 0$, also ist die Gleichung $f(x) = 0$ auch durch den zu x_1 in Bezug auf $\sqrt{r_\alpha}$ conjugirten Wert x_2 zu befriedigen. Die Gleichungen $A = 0$, $B = 0$ nehmen in Bezug auf die vorletzte Wurzel $\sqrt{r_{\alpha-1}}$ die Form an: $A_1 + B_1\sqrt{r_{\alpha-1}} = 0$, $C_1 + D_1\sqrt{r_{\alpha-1}} = 0$, woraus ebenso folgt, dass $A_1 = 0$, $B_1 = 0$, $C_1 = 0$, $D_1 = 0$ sein muss, dass also auch die zu x_1 und x_2 in Bezug auf $\sqrt{r_{\alpha-1}}$ conjugirten Werte x_3 und x_4 die Gleichung $f(x) = 0$ befriedigen, u. s. w. Die sämmtlichen Wurzeln von $f(x) = 0$ ordnen sich also in Gruppen von 2^α conjugirten, $2^{\alpha'}$ conjugirten, u. s. w. Jetzt sind offenbar $x_1 + x_2$, x_1x_2, $x_3 + x_4$, x_3x_4, .. rational in $\sqrt{r_1}, \ldots, \sqrt{r_{\alpha-1}}$; also $x_1 + x_2 + x_3 + x_4$, $(x_1 + x_2)(x_3 + x_4)$, $x_1x_2 + x_3x_4$, $x_1x_2x_3x_4$, .. rational in $\sqrt{r_1}, \ldots, \sqrt{r_{\alpha-2}}$ u. s. w., und ebenso für die Gruppen von $2^{\alpha'}$ conjugirten Wurzeln u. s. w., u. s. w.; woraus schliesslich hervorgeht, dass die mit $x^{(1)}, \ldots, x^{(n)}$ bezeichneten Funktionen, also auch u rational ist; w. z. b. w. Wir können daher den Satz aussprechen:

Damit eine von ihren Doppelwurzeln befreite Gleichung $f(x) = 0$ durch Quadratwurzeln vollkommen auflösbar sei, ist nothwendig und hinreichend, dass ihre Resolvente $G(u) = 0$ eine rationale Wurzel habe.

6. Für eine kubische Gleichung ohne Doppelwurzel ergiebt sich ohne weiteres, dass, wenn sich nur *eine* Wurzel durch Quadratwurzeln darstellen lässt, dasselbe für eine zweite der Fall ist, während die dritte rational wird. Die Resolvente $G(u) = 0$ hat die drei Wurzeln: $u = u_1 x_1 + u_2(x_2 + x_3) + u_3 x_2 x_3$ und stimmt für die zulässige Wahl $u_1 = 1$, $u_2 = 0$, $u_3 = 0$ mit der kubischen Gleichung selbst überein. Also:

Damit sich eine Wurzel einer kubischen Gleichung durch Quadratwurzeln darstellen lässt, ist notwendig und hinreichend, dass die kubische Gleichung eine rationale Wurzel besitzt.

7. Nur für $n = 4$ ist N kleiner als n, nämlich gleich drei: man erhält die Auflösung der biquadratischen Gleichung durch eine kubische Resolvente. Sind x_1, x_2, x_3, x_4 die Wurzeln der Gleichung:

$$ax^4 + 4bx^3 + 6cx^2 + 4dx + e = 0, \qquad (a=1)$$

so hat die Resolvente:

$$4u^3 - (ae - 4bd + 3c^2)u + (ace + 2bcd - ad^2 - c^3 - b^2 e) = 0$$

die Wurzeln:

$$u = \frac{1}{6}(x_1 x_2 + x_3 x_4) - \frac{1}{6}(x_1 + x_2)(x_3 + x_4).$$

Aus den daraus folgenden Gleichungen:

$$x_1 x_2 + x_3 x_4 = 3c + 3u \qquad (x_1 + x_2)(x_3 + x_4) = 3c - 3u$$

$$x_1 x_2 x_3 x_4 = e \qquad x_1 + x_2 + x_3 + x_4 = -4b$$

ergiebt sich:

$$\left.\begin{matrix} x_1 x_2 \\ x_3 x_4 \end{matrix}\right\} = \frac{3c + 3u}{2} \pm \sqrt{\frac{9}{4}(c + u)^2 - e}, \qquad \left.\begin{matrix} x_1 + x_2 \\ x_3 + x_4 \end{matrix}\right\} = -2b \pm \sqrt{4b^2 - 3(c - u)}.$$

Die Vorzeichen gehören so zusammen, dass:

$$x_1 x_2 (x_3 + x_4) + x_3 x_4 (x_1 + x_2) = -4d, \text{ d. h.}$$

$$\sqrt{\frac{9}{4}(c+u)^2 - e} \, . \, \sqrt{4b^2 - 3(c-u)} = -2d + 3b(c+u)$$

ist; dann ergeben sich die vier Wurzeln aus der Formel:

$$-b \pm \sqrt{b^2 - \frac{3}{4}(c-u)}$$

$$\pm \sqrt{\left(-b \pm \sqrt{b^2 - \frac{3}{4}(c-u)}\right)^2 - \frac{3}{2}(c+u) \pm \sqrt{\frac{9}{4}(c+u)^2 - e}},$$

welche die Cartesische verallgemeinert und aus der unmittelbar der Satz ersichtlich ist: *Eine biquadratische Gleichung ist dann und nur dann durch Quadratwurzeln auflösbar, wenn ihre kubische Resolvente eine rationale Wurzel hat.*

8. Die Rationalität der durch u repräsentirten Affektfunktionen kann bei besonderen Eigenschaften der Gleichung $f(x) = 0$ manchmal direkt erkannt werden. Es sei z. B. $p = 2^\alpha + 1$ eine Primzahl, $f(x) = \frac{x^p - 1}{x - 1}$, x eine Wurzel von $f(x) = 0$, g eine primitive Wurzel für p. Setzt man:

$$x^{g^{i_0 + 2i_1 + 2^2 i_2 + \ldots + 2^{\alpha-1} i_{\alpha-1}}} = x_{2^{\alpha-1} i_0 + 2^{\alpha-2} i_1 + \ldots + i_{\alpha-1}}, \qquad (i_0, \ldots, i_{\alpha-1} = 0, 1)$$

so sind $x_0, x_1, \ldots, x_{2^\alpha - 1}$ alle Wurzeln von $f(x) = 0$. Jetzt sei $(x_0 x_1)$ eine rationale symmetrische Funktion von x_0 und x_1, $(x_2 x_3)$ dieselbe Funktion von x_2 und x_3; $(x_0 x_1 x_2 x_3)$ eine rationale symmetrische Function von $(x_0 x_1)$ und $(x_2 x_3)$; $(x_4 x_5 x_6 x_7)$ dieselbe Funktion von x_4, x_5, x_6, x_7, u. s. w., so ist:

$$(x_0 x_1 x_2 x_3 \ldots x_{2^\alpha - 1})$$

eine rationale Function von x, welche offenbar bei jeder Substitution:

$$x \,\|\, x^{g^{2^\beta}}, \qquad (\beta = 0, 1, \ldots, \alpha - 1)$$

also auch bei jeder aus diesen componirten Substitution:

$$x \| x^{g^i} \qquad {\scriptstyle (i=0,1,..,2^{\alpha}-1)}$$

unverändert bleibt, also rational ist. Also:

Die Kreistheilungsgleichung $x^p = 1$ ist durch Quadratwurzeln auflösbar oder das reguläre p-Eck ist mit Zirkel und Lineal construirbar, wenn p eine Primzahl von der Form $2^{\alpha} + 1$ ist.

9. Im Allgemeinen, wo $G(u)$ keine rationale Wurzel besitzt, ergiebt sich für eine Gleichung $f(x) = 0$ mit *reellen Zahlencoëfficienten* die Existenz und Ermittelung sämmtlicher Wurzeln aus dem Umstande, dass die Gleichung $G(u) = 0$ reelle Coëfficienten und *ungraden* Grad, also sicher eine — reelle — Wurzel besitzt. Dieser Beweis des *Fundamentalsatzes der Algebra* schliesst sich an die mit Euler und de Foncenex beginnende Gruppe von Beweisen an und wird, wie fast alle diese, von dem Gaussischen Einwand betroffen: es werde dabei die Wurzelexistenz bereits vorausgesetzt. Auf die Berechtigung oder Nichtberechtigung dieses Einwandes soll an dieser Stelle nicht näher eingegangen, sondern nur gezeigt werden, dass ohne Überwindung principieller Schwierigkeiten dem Beweise eine von diesem Einwande freie Form gegeben werden kann.

10. Zunächst ist Folgendes vorauszuschicken:

Es sei $f(x)$ eine ganze Funktion, $f'(x)$ ihre Ableitung. Durch das Euklidische Verfahren werde ihr höchster gemeinsamer Teiler:

$$f_1 = (f, f')$$

gefunden; ebenso sei

$$f_2 = (f_1, f_1')$$

u. s. w. bis zu

$$f_r = (f_{r-1}, f'_{r-1}) = \text{const.}.$$

Dann giebt in der Reihe *ganzer* Funktionen:

$$\frac{f}{f_1}, \frac{f_1}{f_2}, \ldots, \frac{f_{r-1}}{f_r}, 1$$

jede, $\frac{f_{i-1}}{f_i}$, dividirt durch die folgende, $\frac{f_i}{f_{i+1}}$, eine *ganze* Funktion g_i, wie aus der Identität hervorgeht:

$$\frac{f'_{i-1}}{f_i} - \left(\frac{f_{i-1}}{f_i}\right)' = \frac{f'_i}{(f_i\,,\,f'_i)} \cdot \frac{f_{i-1}f_{i+1}}{f_i^2}\,; \qquad \binom{i=1,2,..,r-1}{f_0=f}$$

da ein Nenner von $\frac{f_{i-1}f_{i+1}}{f_i^2}$ ein Faktor von f_i^2 wäre, also zwar in f'_i, aber nicht mehr in $\frac{f'_i}{(f_i\,,\,f'_i)}$ enthalten sein könnte. Also wird: $\frac{f_{i-1}}{f_i} = g_i g_{i+1}, \ldots g_r$ und daraus $f_{i-1} = g_i g_{i+1}^2 g_{i+2}^3 \ldots g_r^{r-i+1}$, speciell $f = g_1 g_2^2 g_3^3 \ldots g_r^r$, wo die Funktionen g_i ganze Funktionen sind. Für diese gilt der Satz:

a) Die Funktionen $g_1, g_2, \ldots, g_r$ sind paarweise teilerfremd und jede ohne mehrfachen Teiler.

Denn enthalten sie einen einfachen Faktor bzw. i_1-, i_2-, .., i_r-mal, so enthält f denselben $(i_1 + 2i_2 + 3i_3 + \ldots + ri_r)$-mal und f', wie die Differentiation zeigt, einmal weniger; aber $f_1 = g_2 g_3^2 \ldots g_r^{r-1}$ enthält ihn $(i_1 + i_2 + \ldots + i_r)$-mal weniger, also muss $i_1 + i_2 + \ldots + i_r = 1$ sein, woraus die Behauptung folgt.

Da also speciell g_1 keinen mehrfachen Teiler hat, folgt aus $f_1 = g_2 g_3^2 \ldots g_{r-1}^r$ der Satz:

b) Eine ganze Funktion hat keinen mehrfachen Teiler wenn und nur wenn sie zu ihrer Ableitung teilerfremd ist.

Aus *a*) und *b*) folgt:

c) Jede Funktion g_i ist zu ihrer Ableitung teilerfremd.

Schliesslich aus *a*) und *c*):

d) Die Auffindung aller Faktoren einer ganzen Funktion, eines jeden gleich in richtiger Vielfachheit, kommt auf die Zerlegung solcher Funktionen zurück, die zu ihrer Ableitung teilerfremd sind.

11. Mit

$$\xi_{i_1,\ldots,i_\alpha} \qquad \begin{pmatrix} (i_1,\ldots,i_\alpha = 0,1) \\ \alpha = \alpha_1,\ldots,\alpha_\nu \\ \alpha_1 > \alpha_2 \ldots > \alpha_\nu \end{pmatrix}$$

werden

$$2^{\alpha_1} + 2^{\alpha_2} + \ldots + 2^{\alpha_\nu} = n$$

unbestimmte Zahlen, mit $\gamma_1, \gamma_2, \ldots, \gamma_n$ die Werte ihrer elementarsymmetrischen Funktionen bezeichnet.

Durch die Gleichungen:

$$\text{I} \qquad \left\{\begin{aligned} \xi^{(0,i_{\beta+1},\ldots,i_a)}_{i_1,\ldots,i_{\beta-1}} &= \xi^{(i_{\beta+1},\ldots,i_a)}_{i_1,\ldots,i_{\beta-1},0} + \xi^{i_{\beta+1},\ldots,i_a)}_{i_1,\ldots,i_{\beta+1},1} \\ \xi^{(1,i_{\beta-1},\ldots,i_a)}_{i_1,\ldots,i_{\beta-1}} &= \xi^{(i_{\beta+1},\ldots,i_a)}_{i_1,\ldots,i_{\beta-1},0} \cdot \xi^{i_{\beta+1},\ldots,i_a)}_{i_1,\ldots,i_{\beta-1},1} \end{aligned}\right. \qquad \begin{pmatrix} i_1,\ldots,i_a = 0,1 \\ \beta = a, a-1, a-2, \ldots, 2, 1 \\ a = a_1, a_2, \ldots, a_r \end{pmatrix}$$

wird ein System ganzer Funktionen der $\xi_{i_1,\ldots,i_a}$ definirt. Setzt man:

$$\omega = \sum \omega_{(i_1,\ldots,i_a)} \xi_{(i_1,\ldots,i_a)} \qquad \begin{pmatrix} i_1\ldots,i_a = 0,1 \\ a = a_1,\ldots,a_\nu \end{pmatrix}$$

mit Unbestimmten $\omega^{(i_1,\ldots,i_a)}$, so bleibt ω ungeändert bei Vertauschung des Systems:

$$\xi_{i_1,\ldots,i_{\beta-1},0,i_{\beta+1},\ldots,i_a} \qquad (i_{\beta+1},\ldots,i_a = 0,1)$$

mit dem Systeme:

$$\xi_{i_1,\ldots,i_{\beta-1},1,i_{\beta+1},\ldots,i_a}, \qquad (i_{\beta+1},\ldots,i_a = 0,1)$$

also, da es $2^{\beta-1}$ solcher Systeme giebt — nämlich für $i_1, i_2, \ldots, i_{\beta-1} = 0, 1$ — im Ganzen bei $2^{\sum_a \sum_\beta 2^{\beta-1}} = 2^{\sum_a 2^{a-1}} = 2^{n-\nu}$ Permutationen der $\xi^{i_1,\ldots,i_a}$. Die Gleichung $G(\omega; \ldots \omega^{(i,\ldots,i_a)} \ldots, \ldots \gamma_i \ldots) = 0$, welcher ω genügt, ist also von dem *ungraden*[1] Grade $N = \frac{|\underline{n}}{2^{n-\nu}}$; ihre Coëfficienten sind *ganze* Funktionen der $\omega^{(i_1,\ldots,i_a)}$ und der γ_i, der höchste Coëfficient ist gleich Eins.

Die Grössen $\xi^{(i_1,\ldots,i_a)}$ sind, im Rationalitetsbereich $(\ldots \omega^{(i_1,\ldots,i_a)} \ldots, \ldots \gamma_i \ldots)$, rationale Funktionen von ω. Durch Auflösung der quadratischen Gleichungen:

$$\text{II} \qquad \left(\xi^{(i_{\beta+1},\ldots,i_a)}_{i_1,\ldots,i_\beta}\right)^2 - \xi^{(0,i_{\beta+1},\ldots,i_a)}_{i_1,\ldots,i_{\beta-1}} \left(\xi^{(i_{\beta+1},\ldots,i_a}_{i_1,\ldots,i_\beta}\right) + \xi^{(1,i_{\beta+1},\ldots,i_a)}_{i_1,\ldots,i_{\beta-1}} = 0 \qquad \begin{pmatrix} i_1,\ldots,i_a = 0,1 \\ \beta = 1, 2, \ldots, a \\ a = a_1, a_2, \ldots, a_\nu \end{pmatrix}$$

---

[1] Bekanntlich enthält $|\underline{n}$ eine Primzahl p genau $\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots = \frac{n - n_p}{p-1}$ mal als Faktor, wenn n_p die Quersumme von n im p adischen Zahlsysteme bedeutet; für $p = 2$ wird die Anzahl gleich $n - \nu$.

ergeben sich die $\xi_{i_1,\dots,i_\alpha}$ als explicite algebraische Funktionen von den $\xi^{(i_1,\dots,i_\alpha)}$, also von ω; die zusammengehörigen Quadratwurzelvorzeichen ergeben sich daraus, dass jedes $\xi^{(i_{\beta+1},\dots,i_\alpha)}_{i_1,\dots,i_\beta}$ rationale Funktion von

III $$\omega_{i_1,\dots,i_\beta} = \sum \omega^{(i_{\beta+1},\dots,i_\alpha)} \xi^{(i_{\beta+1},\dots,i_\alpha)}_{i_1,\dots,i_\beta} \qquad (i_{\beta+1},\dots,i_\alpha=0,1)$$

ist, wo die Unbestimmten $\omega^{(i_{\beta+1},\dots,i_\alpha)}$ in den Rationalitätsbereich aufzunehmen sind.

Wir wollen die Permutationen der $\xi_{i_1,\dots,i_\alpha}$, bei welchen ω ungeändert bleibt, als die Gruppe (ω) bezeichnen. Die Grösse $\omega_{i_1,\dots,i_\beta}$ nimmt bei den Permutationen der Gruppe (ω) die 2^β conjugirten Werte:

$$\omega_{i_1,\dots,i_\beta} \qquad (i_1,\dots,i_\beta=0,1)$$

an. Es sei $\bar{\xi}_{i_1,\dots,i_\alpha}$ eine nicht zur Gruppe (ω) gehörige Permutation der $\xi_{i_1,\dots,i_\alpha}$ und $\bar{\omega},\dots$ die den $\omega,\dots$ analogen Funktionen. Eine Unbestimmtheit in den Ausdrücken der $\xi_{i_1,\dots,i_\alpha}$ durch ω kann nur eintreten, wenn z. B.

$$\omega_{i_1,\dots,i_\beta} = \bar{\omega}_{i'_1,\dots,i'_\beta}$$

ist. Durch blosse Bezeichnungsänderung in den Indices der $\bar{\xi}_{i_1,\dots,i_\alpha}$ ergiebt sich statt dessen:

$$\omega_{i_1,\dots,i_\beta} = \bar{\omega}_{i_1,\dots,i_\beta},$$

woraus das System:

$$\xi^{(i_{\beta+1},\dots,i_\alpha)}_{i_1,\dots,i_\beta} = \bar{\xi}^{(i_{\beta+1},\dots,i_\alpha)}_{i_1,\dots,i_\beta} \qquad (i_{\beta+1},\dots,i_\alpha=0,1)$$

folgt. Die Gleichungen II ergeben dann:

$$\xi_{i_1,\dots,i_\alpha} = \bar{\xi}_{i_1,\dots,i_\alpha}, \qquad \begin{pmatrix} i_1,\dots,i_\alpha=0,1 \\ \alpha=\alpha_1,\alpha_2,\dots,\alpha_\nu \end{pmatrix}$$

abgesehen von Permutationen der Gruppe (ω). Da sich die Reihenfolgen $\xi_{i_1,\dots,i_\alpha}$ und $\bar{\xi}_{i_1,\dots,i_\alpha}$ nicht nur durch solche Permutationen unterscheiden sollen, müssen wenigstens zwei der Grössen $\xi_{i_1,\dots,i_\alpha}$ zusammenfallen. Daraus folgt umgekehrt, dass auch zwei der N Werte von ω zusammenfallen.

12. Das Produkt der $N(N-1)$ Wurzeldifferenzen von

$$G(\omega\,;\,..\,\omega^{(i_1,..,i_\alpha)}\,..\,,\,..\,\gamma_i\,..)=0$$

ist eine ganze Funktion $D(..\,\omega^{(i_1,..,i_\alpha)}\,..\,,\,\gamma_i\,..)$, deren höchster von den $\omega^{(i_1,..,i_\alpha)}$ unabhängiger Faktor $\Delta(..\,\gamma_i\,..)$ sei. Geben wir jetzt den Zahlen γ_i specielle reelle Werte c_i, so dass $\Delta(..\,c_i\,..)\neq 0$ ist, so kann man auch den $\omega^{(i_1,..,i_\alpha)}$ solche reellen Werte $u^{(i_1,..,i_\alpha)}$ geben, dass $D(..\,u^{(i_1,..,i_\alpha)},.,..\,c_i..)\neq 0$ ist. Auch den in III vorkommenden Unbestimmten $\omega^{(i_{\beta+1},..,i_\alpha)}$ sind solche reellen Werte $u^{(i_{\beta+1},..,i_\alpha)}$ beizulegen, dass die Discriminanten der Gleichungen für die $\omega_{i_1,..,i_\beta}$ nicht verschwinden. Wir definiren jetzt ω als *eindeutige* Funktion der reellen Veränderlichen $..\,\gamma_i\,..$ durch folgenden Algorithmus: durch eventuelle Substitution $\omega \,\|\, -\omega$ wird bewirkt, dass $G(\omega\,;..\,u^{(i_1,..,i_\alpha)}..,..\,\gamma_i..)$ im Intervall $\frac{0}{1}\,..\,\frac{1}{0}$ das Vorzeichen wechselt; jedes Intervall $\frac{a}{b}\,..\,\frac{c}{d}$ in welchem $G(\omega\,;\,..)$ das Zeichen wechselt, werde durch $\frac{a+c}{b+d}$ in zwei kleinere geteilt, in deren einem der Wechsel erfolgt; so kann man von $\frac{0}{1}\,..\,\frac{1}{0}$ ausgehend eine *bestimmte* Wurzel von $G(\omega\,;\,..)$ in beliebig enge Grenzen einschliessen.[1] Nun ist jedes $\xi_{i_1,..,i_\alpha}$ rational in $\omega_{i_1,..,i_\alpha}$; jedes $\omega_{i_1,..,i_\alpha}$ von der Form $A+(-1)^{i_\beta}\sqrt{B}$, wo A und B rational in $\omega_{i_1,..,i_{\beta-1}}$ sind. Dadurch wird jede der n Zahlen $\xi_{i_1,..,i_\alpha}$ eine vollkommen bestimmte Funktion der Werte der elementarsymmetrischen Funktionen γ_i; und das ganze Verfahren versagt dann und nur dann, wenn die γ_i solche speciellen Werte annehmen, dass

$$D(..\,u^{(i_1,..,i_\alpha)}\,..\,,\,..\,\gamma_i\,..)=0$$

ist. Dies findet für die Annahme $\gamma_i=c_i$ nicht statt; erhalten in diesem Falle die $\xi_{i_1,..,i_\alpha}$ die Werte $x_{i_1,..,i_\alpha}$, so haben sich uns diese Werte, für welche:

$$x^n-c_1x^{n-1}+c_2x^{n-2}-\,..\,c_n=\Pi\,(x-x_{i_1,..,i_\alpha})$$

ist, ergeben, *ohne ihre Existenz vorauszusetzen.* Die Bedingung:

$$D(..\,u^{(i_1,..,i_\alpha)}\,..\,,\,..\,c_i\,..)\neq 0,$$

[1] Stösst man auf eine rationale Wurzel, so nehme man diese.

unter welcher die Ermittelung der $x_{i_1,..,i_a}$ nur stattfinden konnte, erweist sich nach (11) als identisch mit der Annahme, dass die $x_{i_1,..,i_a}$ alle von einander verschieden sind, oder dass $f(x) = x^n - c_1 x^{n-1} + \ldots \nu c_n$ keinen mehrfachen Teiler besitzt; und diese ist nach (10b) erfüllt, wenn und nur wenn $f(x)$ und $f'(x)$ teilerfremd sind, wie nach (10 d) vorausgesetzt werden durfte.

Damit ist der Beweis des Fundamentalsatzes vollendet. Derselbe vereinigt — allen anderen Beweisen gegenüber — die drei Vorzüge in sich:

erstens: nur arithmetisch-algebraische Hilfsmittel und zwar der einfachsten Art zu benutzen,

zweitens: *die* Grössen wirklich zu ermitteln, deren Existenz er nachweist,

drittens: sich gleichzeitig auf *sämmtliche* Wurzeln zu beziehen.