

Beweis der Unmöglichkeit algebraische Gleichungen von höheren Graden als dem vierten allgemein aufzulösen.

(Von Herrn N. H. Abel.)

Bekanntlich kann man algebraische Gleichungen bis zum vierten Grade allgemein auflösen, Gleichungen von höhern Graden aber nur in einzelnen Fällen, und irre ich nicht, so ist die Frage:

Ist es *möglich*, Gleichungen von höhern als dem vierten Grade allgemein aufzulösen?

noch nicht befriedigend beantwortet worden. Der gegenwärtige Aufsatz hat diese Frage zum Gegenstande.

Eine Gleichung algebraisch auflösen heißt nichts anders, als ihre Wurzeln durch eine algebraische Function der Coefficienten ausdrücken. Man muß also erst die allgemeine *Form* algebraischer Functionen betrachten und alsdann untersuchen, ob es möglich sei, der gegebenen Gleichung auf die Weise genug zu thun, daß man den Ausdruck einer algebraischen Function statt der unbekannten Größe setzt.

§. I. Ueber die allgemeine Form algebraischer Functionen.

Wenn $x', x'', x''' \dots$ eine endliche Menge beliebiger Größen sind, so sagt man: ϱ sei eine algebraische Function dieser Größen, wenn es sich durch $x', x'', x''' \dots$ etc. mittelst folgender Operationen ausdrücken läßt. *Erstlich* durch die *Addition*, *zweitens* durch die *Multiplication*, sowohl von Größen, die von $x', x'', x''' \dots$ abhängen, als von Größen, die nicht davon abhängen; *drittens* durch die *Division*; viertens durch *Ausziehen von Wurzeln* mit Exponenten, die Primzahlen sind. Wir nennen die *Subtraction*, *Potenzirung* und *Ausziehung von Wurzeln* mit zusammengesetzten Exponenten nicht besonders, weil sie offenbar in den vier vorhin genannten Operationen mit enthalten sind.

Läßt sich die Function ϱ durch die drei ersten der vier obigen Operationen zusammensetzen, so ist sie *algebraisch rational* oder bloß rational; und

sind nur die beiden ersten Operationen nöthig, so heißt sie *algebraisch-rational* und *ungebrochen*, oder auch bloß *ganze* Function.

Es sei $f(x', x'', x''' \dots)$ eine beliebige Function, welche durch die Summe einer endlichen Zahl von Gliedern von der Form

$$A x'^{m_1} x''^{m_2} \dots$$

ausgedrückt werden kann, wo A eine von $x', x'' \dots$ unabhängige Größe ist, und $m_1, m_2 \dots$ ganze positive Zahlen bedeuten; so ist klar, daß die zwei ersten obigen Operationen besondere Fälle der durch $f(x', x'' \dots)$ bezeichneten Operation sind. Man kann also *ganze* Functionen, ihrer Definition zufolge, als aus einer endlichen Zahl von Wiederholungen dieser Operationen entstehend betrachten. Bezeichnet man nun durch $\varrho', \varrho'', \varrho''' \dots$ mehrere Functionen der

Größen $x', x'', x''' \dots$ von der nämlichen Form wie $f(x', x'' \dots)$, so ist auch offenbar $f(\varrho', \varrho'', \varrho''' \dots)$ eine Function von eben der Form wie $f(x', x'' \dots)$. Nun ist $f(\varrho', \varrho'' \dots)$ der allgemeine Ausdruck der Functionen, welche durch zweimalige Wiederholung der Operation $f(x', x'' \dots)$ entstehen. Man findet also auch immer das nämliche Resultat, wenn man die Operation beliebig oft wiederholt. Daraus folgt, daß jede ganze Function mehrerer Größen $x', x'' \dots$ durch die Summe mehrerer Glieder von der Form $Ax'^{m_1}x''^{m_2} \dots$ ausgedrückt werden kann.

Wir wollen nunmehr die rationalen Functionen betrachten.

Wenn $f(x', x'' \dots)$ und $\varphi(x', x'' \dots)$ zwei ganze Functionen sind, so ist klar, daß der Quotient

$$\frac{f(x', x'' \dots)}{\varphi(x', x'' \dots)}$$

ein besonderer Fall der Resultate der drei ersten Operationen ist, welche rationale Functionen geben. Man kann also eine rationale Function als das Resultat der Wiederholung dieser Operation betrachten. Bezeichnet man durch $\varrho', \varrho'', \varrho'''$ etc. mehrere Functionen von der Form $\frac{f(x', x'' \dots)}{\varphi(x', x'' \dots)}$, so ist leicht zu sehen, daß

$\frac{f(\varrho', \varrho'' \dots)}{\varphi(\varrho', \varrho'' \dots)}$ wiederum auf die nämliche Form gebracht werden kann. Es folgt also, wie oben bei den ungebrochenen Functionen, daß jede rationale Function von mehreren Größen $x', x'' \dots$ immer auf die Form

$$\frac{f(x', x'' \dots)}{\varphi(x', x'' \dots)}$$

gebracht werden kann, wo Zähler und Nenner ganze Functionen sind.

Wir wollen ferner die *allgemeine* Form algebraischer Functionen suchen.

Man bezeichne durch $f(x', x'' \dots)$ eine beliebige rationale Function, so ist klar, daß jede algebraische Function mittelst der durch $f(x', x'' \dots)$ bezeichneten Operation, verbunden mit der Operation $\sqrt[m]{r}$, wo m eine Primzahl ist, zusammengesetzt werden kann. Sind also $p', p'' \dots$ rationale Functionen von $x', x'' \dots$, so wird

$$p_1 = f(x', x'' \dots \sqrt[n']{p'}, \sqrt[n'']{p''} \dots)$$

die allgemeine Form algebraischer Functionen von $x', x'' \dots$ sein, in welchen sich die durch $\sqrt[n]{r}$ ausgedrückte Operation nunmehr nur auf rationale Functionen bezieht. Wir wollen die Functionen von der Form p_1 algebraische Functionen *von der ersten Ordnung* nennen. Bezeichnet man durch p'_1, p''_1 etc. mehrere Größen von der Form p_1 , so wird

$$p_2 = f(x', x'' \dots \sqrt[n']{p'}, \sqrt[n'']{p''} \dots \sqrt[n'_1]{p'_1}, \sqrt[n''_1]{p''_1} \dots)$$

die allgemeine Form algebraischer Functionen von $x', x'' \dots$ sein, in welchen die Operation $\sqrt[n]{r}$ sich nur auf rationale und auf algebraische Functionen *von der ersten Ordnung* bezieht. Wir wollen die Functionen von der Form p_2 algebraische Functionen *von der zweiten Ordnung* nennen. Auf dieselbe Weise wird der Ausdruck

$$p_3 = f(x', x'' \dots \sqrt[n']{p'}, \sqrt[n'']{p''} \dots \sqrt[n'_1]{p'_1}, \sqrt[n''_1]{p''_1} \dots \sqrt[n'_2]{p'_2}, \sqrt[n''_2]{p''_2} \dots),$$

in welchem p'_2, p''_2 Functionen der zweiten Ordnung sind, die allgemeine Form algebraischer Functionen von $x', x'' \dots$ sein, in welchen die Operation $\sqrt[\mu]{r}$ sich nur auf rationale und auf algebraische Functionen der ersten und zweiten Ordnung bezieht.

Führt man auf diese Weise fort, so bekommt man algebraische Functionen von der *dritten, vierten* $\dots \mu^{\text{ten}}$ Ordnung, und es ist klar, daß der Ausdruck der Functionen von der μ^{ten} Ordnung der *allgemeine* Ausdruck algebraischer Functionen sein wird.

Bezeichnet man also durch μ die Ordnungszahl einer beliebigen algebraischen Function und durch ϱ die Function selbst, so ist

$$\varrho = f(r', r'' \dots \sqrt[n']{p'}, \sqrt[n'']{p''} \dots),$$

wo $p', p'' \dots$ Functionen von der Ordnung $\mu - 1$; $r', r'' \dots$ Functionen von der Ordnung $\mu - 1$, oder niedrigen Ordnungen, und $n', n'' \dots$ Primzahlen sind. f bezeichnet, wie immer, eine rationale Function der Größen, welche zwischen den Klammern stehen.

Man kann offenbar annehmen, daß es unmöglich ist, eine der Größen $\sqrt[n']{p'}, \sqrt[n'']{p''} \dots$ durch eine rationale Function der übrigen und der Größen $r', r'' \dots$ auszudrücken; denn wäre es möglich, so würde ϱ die einfachere Gestalt

$$\varrho = f(r', r'' \dots \sqrt[n']{p'}, \sqrt[n'']{p''} \dots)$$

haben, wo die Zahl der Größen $\sqrt[n']{p'}, \sqrt[n'']{p''} \dots$ wenigstens um eine Einheit geringer wäre wie oben. Reducirte man nun, wenn es angeht, diesen Ausdruck von ϱ eben so noch weiter, so müßte man zuletzt nothwendig entweder auf einen irreductibeln Ausdruck, oder auf einen Ausdruck von der Form

$$\varrho = f(r', r'', r''' \dots)$$

kommen. Diese Function wäre aber bloß von der $\mu - 1^{\text{ten}}$ Ordnung, während ϱ von der μ^{ten} Ordnung sein sollte; welches sich widerspricht.

Ist in dem Ausdruck von ϱ die Zahl der Größen $\sqrt[n']{p'}, \sqrt[n'']{p''} \dots$ gleich m , so wollen wir die Function ϱ von der μ^{ten} *Ordnung* und vom m^{ten} *Grade* nennen. Auf diese Weise ist eine Function von der μ^{ten} Ordnung und vom 0^{ten} Grade das nemliche, wie eine Function von der $\mu - 1^{\text{ten}}$ Ordnung, und eine Function von der 0^{ten} Ordnung ist das nämliche wie eine *rationale* Function.

Daraus folgt, daß man setzen kann

$$\varrho = f(r', r'' \dots \sqrt[\mu]{p})$$

wo p eine Function von der $\mu - 1^{\text{ten}}$ Ordnung ist, $r', r'' \dots$ aber Functionen von der μ^{ten} Ordnung und höchstens vom $m - 1^{\text{ten}}$ Grade und von der Art sind, daß es unmöglich ist, $\sqrt[\mu]{p}$ durch eine rationale Function dieser Größen auszudrücken.

Da eine rationale Function mehrerer Größen, wie wir vorhin sahen, immer auf die Form

$$\frac{s}{t}$$

gebracht werden kann, wo s und t ganze Functionen der nemlichen veränderlichen Größen sind, so kann ϱ immer durch

$$\varrho = \frac{\varphi(r', r'' \dots \sqrt[n]{p})}{\tau(r', r'' \dots \sqrt[n]{p})}$$

ausgedrückt werden, wo φ und τ zwei ganze Functionen der Größen $r', r'' \dots$ und $\sqrt[n]{p}$ bezeichnen. Vermöge dessen, was wir oben fanden, kann aber eine ganze Function mehrer Größen $s, r', r'' \dots$ immer durch¹

$$t_0 + t_1 s^1 + t_2 s^2 \dots t_m s^m)$$

ausgedrückt werden, wenn $t_0, t_1 \dots t_m$ ganze Functionen von $r', r'', r''' \dots$ ohne s bedeuten. Man kann also

$$\varrho = \frac{t_0 + t_1 p^{\frac{1}{n}} + t_2 p^{\frac{2}{n}} \dots t_m p^{\frac{m}{n}}}{\varrho_0 + \varrho_1 p^{\frac{1}{n}} + \varrho_2 p^{\frac{2}{n}} \dots \varrho_{m'} p^{\frac{m'}{n}}} = \frac{T}{V}$$

setzen, wo $t_0, t_1 \dots t_m$ und $\varrho_0, \varrho_1 \dots \varrho_{m'}$ ganze Functionen von $r', r'', r''' \dots$ sind.

Nun mögen $V_1, V_2 \dots V_{n-1}$ die $n-1$ Werthe von V sein, welche man findet, wenn man $\alpha \cdot p^{\frac{1}{n}}, \alpha^2 p^{\frac{1}{n}}, \alpha^3 p^{\frac{1}{n}} \dots \alpha^{n-1} p^{\frac{1}{n}}$ statt $p^{\frac{1}{n}}$ setzt: α bedeutet eine der Wurzeln der Gleichung $\alpha^n - 1 = 0$, die nicht 1 ist. Alsdann erhält man, wenn man den Bruch $\frac{T}{V}$ oben und unten mit

$V_1 V_2 \dots V_{n-1}$ multiplicirt,

$$\varrho = \frac{T \cdot V_1 \cdot V_2 \dots V_{n-1}}{V \cdot V_1 \cdot V_2 \dots V_{n-1}}.$$

Das Product $V \cdot V_1 \dots V_{n-1}$ kann aber, wie bekannt, durch eine ganze Function von p und von den Größen $r', r'' \dots$ ausgedrückt werden, und das Product $T \cdot V_1 \cdot V_2 \dots V_{n-1}$ ist, wie man sieht, eine ganze Function von $\sqrt[n]{p}$ und $r', r'' \dots$. Setzt man also dieses Product gleich

$$s_0 + s_1 p^{\frac{1}{n}} + s_2 p^{\frac{2}{n}} \dots s_k p^{\frac{k}{n}},$$

so findet man

$$\varrho = \frac{s_0 + s_1 p^{\frac{1}{n}} + s_2 p^{\frac{2}{n}} \dots s_k p^{\frac{k}{n}}}{M},$$

oder, wenn man $q_0, q_1, q_2 \dots$ statt $\frac{s_0}{m}, \frac{s_1}{m}, \frac{s_2}{m}$ etc. schreibt,

$$\varrho = q_0 + q_1 p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} \dots + q_k p^{\frac{k}{n}},$$

wo $q_0, q_1 \dots q_k$ rationale Functionen der Größen $p, r', r'' \dots$ sind. Welche nun auch die ganze Zahl μ sein mag, so kann man setzen

$$\mu = an + \alpha,$$

¹*Editorial note:* The following display closes with a parenthesis that has no matching opening parenthesis in the print — an apparent typographical slip, reproduced here as printed.

wo a und α zwei ganze Zahlen sind und $\alpha < n$ ist. Daraus folgt, daß

$$p^{\frac{\mu}{n}} = p^{\frac{an+\alpha}{n}} = p^a \cdot p^{\frac{\alpha}{n}}.$$

Setzt man daher in den Ausdruck von ϱ , statt $p^{\frac{\mu}{n}}$ diesen Ausdruck, so erhält man

$$\varrho = q_0 + q_1 p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} \dots + q_{n-1} p^{\frac{n-1}{n}},$$

wo q_0, q_1, q_2 etc., wie vorhin, rationale Functionen von $p, r', r'' \dots$ und folglich Functionen von der μ^{ten} Ordnung und höchstens vom $m-1^{\text{ten}}$ Grade und von der Art sind, daß sich $p^{\frac{1}{n}}$ nicht durch rationale Functionen dieser Größen ausdrücken läßt.

In dem obigen Ausdruck von ϱ kann man immer

$$q_1 = 1$$

setzen. Denn wenn q_1 nicht Null ist, so erhält man, wenn man $p_1 = p \cdot q_1^n$ setzt,

$$p = \frac{p_1}{q_1^n}, \text{ und } p^{\frac{1}{n}} = \frac{p_1^{\frac{1}{n}}}{q_1}, \text{ also}$$

$$\varrho = q_0 + p_1^{\frac{1}{n}} + \frac{q_2}{q_1^2} p_1^{\frac{2}{n}} \dots + \frac{q_{n-1}}{q_1^{n-1}} p_1^{\frac{n-1}{n}},$$

welcher Ausdruck von der nemlichen Gestalt ist, wie der vorige, nur daß $q_1 = 1$. Ist $q_1 = 0$, so sei q_μ eine von den Größen $q_1, q_2 \dots q_{n-1}$, welche nicht Null ist und $q_\mu^n p^\mu = p_1$. Dieses giebt $q_\mu^\alpha \cdot p^{\frac{\alpha\mu}{n}} = p_1^{\frac{\alpha}{n}}$. Nimmt man daher zwei ganze Zahlen α und β , welche der Gleichung $\alpha\mu - \beta n = \mu'$ genuehthun, wo μ' eine ganze Zahl ist, so erhält man

$$q_\mu^\alpha p^{\frac{\beta n + \mu'}{n}} = p_1^{\frac{\alpha}{n}} \text{ und } p^{\frac{\mu'}{n}} = q_\mu^{-\alpha} \cdot p^{-\beta} \cdot p_1^{\frac{\alpha}{n}}.$$

Diesem zufolge und weil $q_\mu p^{\frac{\mu}{n}} = p_1^{\frac{1}{n}}$ ist, wird ϱ die Form

$$\varrho = q_0 + p_1^{\frac{1}{n}} + q_2 p_1^{\frac{2}{n}} \dots q_{n-1} p_1^{\frac{n-1}{n}}$$

haben.

Aus allem diesen folgt Nachstehendes:

Wenn ϱ eine algebraische Function von der Ordnung μ und vom Grade m ist, so kann man immer setzen:

$$\varrho = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + q_3 p^{\frac{3}{n}} \dots q_{n-1} p^{\frac{n-1}{n}};$$

n ist eine Primzahl, $q_0, q_2 \dots q_{n-1}$ sind algebraische Functionen von der Ordnung μ und höchstens vom Grade $m-1$ und p ist eine algebraische Function von der Ordnung $\mu-1$ und von der Art, daß sich $p^{\frac{1}{n}}$ nicht durch eine rationale Function von $q_0, q_2 \dots q_{n-1}$ ausdrücken läßt.

§. II. Eigenschaften der algebraischen Functionen, welche einer gegebenen Gleichung genugthun.

Es sei

$$c_0 + c_1y + c_2y^2 \dots + c_{r-1}y^{r-1} + y^r = 0 \quad (1)$$

eine beliebige Gleichung vom Grade r , wo $c_0, c_1 \dots$ rationale Functionen von $x', x'' \dots$ sind. $x', x'' \dots$ sind beliebige unabhängige Größen. Man nehme an, es lasse sich derselben genugthun, wenn man statt y irgend eine *algebraische Function* von $x', x'', \dots$ setzt. Diese Function sei

$$y = q_0 + p^{\frac{1}{n}} + q_2p^{\frac{2}{n}} \dots + q_{n-1}p^{\frac{n-1}{n}} \quad (2)$$

Substituirt man diesen Ausdruck von y in die gegebene Gleichung, so erhält man, dem Obigen zufolge, einen Ausdruck von der Form

$$r_0 + r_1p^{\frac{1}{n}} + r_2p^{\frac{2}{n}} \dots + r_{n-1}p^{\frac{n-1}{n}} = 0 \quad (3)$$

wo $r_0, r_1, r_2 \dots r_{n-1}$ rationale Functionen der Größen $p, q_0, q_1 \dots q_{n-1}$ sind.

Nun behaupte ich, daß die Gleichung (3) nicht Statt finden kann, wenn nicht einzeln

$$r_0 = 0, r_1 = 0 \dots r_{n-1} = 0$$

ist. Denn es sei nicht so, so müßten, wenn man z. B. $p^{\frac{1}{n}}$ durch z bezeichnet, die beiden Gleichungen

$$z^n - p = 0 \text{ und}$$

$$r_0 + r_1z + r_2z^2 \dots + r_{n-1}z^{n-1} = 0$$

eine oder mehrere *gemeinschaftliche Wurzeln* haben. Es sei k die Zahl dieser Wurzeln, so läßt sich, wie bekannt, eine Gleichung finden, welche diese k Wurzeln hat und deren Coefficienten rationale Functionen der Größen $p, r_0, r_1 \dots r_{n-1}$ sind.

Die Gleichung sei

$$s_0 + s_1z + s_2z^2 \dots + s_{k-1}z^{k-1} + z^k = 0$$

und

$$t_0 + t_1z + t_2z^2 \dots + t_{\mu-1}z^{\mu-1} + z^\mu$$

ein Factor ihres ersten Gliedes, wo t_0, t_1 etc. rationale Functionen von $p, r_0, r_1 \dots r_{n-1}$ sind, so ist auch²

$$t_0 + t_1z + t_2z \dots + t_{\mu-1}z^{\mu-1} + z^\mu = 0,$$

und es ist klar, daß man es als unmöglich annehmen kann, eine Gleichung von niedrigerem Grade von der nemlichen Form zu finden. Diese Gleichung hat nun ihre μ Wurzeln mit der Gleichung $z^n - p$ gemein. Nun aber sind die Wurzeln

²*Editorial note:* In the following display the third term is printed t_2z without an exponent; by the line just above it should read t_2z^2 . An apparent misprint, reproduced here as printed.

der Gleichung $z^n - p$ alle von der Form αz , wo α irgend eine Wurzel der Einheit ist. Erwägt man also, daß μ nicht kleiner sein kann als 2, weil es unmöglich sein soll, z durch eine rationale Function der Größen $p, r_0, r_1 \dots r_{n-1}$ auszudrücken, so folgt, daß zwei Gleichungen von der Form

$$t_0 + t_1 z + t_2 z^2 \dots + t_{\mu-1} z^{\mu-1} + z^\mu = 0 \text{ und} \\ t_0 + \alpha t_1 z + \alpha^2 t_2 z^2 \dots + \alpha^{\mu-1} t_{\mu-1} z^{\mu-1} + \alpha^\mu z^\mu = 0$$

Statt finden müssen. Aus diesen Gleichungen folgt, wenn man z^μ eliminirt,

$$t_0(1 - \alpha^\mu) + t_1(\alpha - \alpha^\mu)z \dots + t_{\mu-1}(\alpha^{\mu-1} - \alpha^\mu)z^{\mu-1} = 0.$$

Da nun aber die Gleichung $z^\mu + t_{\mu-1}z^{\mu-1} \dots = 0$ irreductibel ist, so muß sie, weil sie vom $\mu - 1^{\text{ten}}$ Grade ist, einzeln

$$\alpha^\mu - 1 = 0, \alpha - \alpha^\mu = 0 \dots \alpha^{\mu-1} - \alpha^\mu = 0$$

geben; was nicht sein kann.

Es muß also

$$r_0 = 0, r_1 = 0 \dots r_{n-1} = 0$$

sein.

Finden nun aber diese Gleichungen Statt, so ist klar, daß der gegebenen Gleichung durch alle die Werthe von y genug gethan werden muß, welche man findet, wenn man der Größe $p^{\frac{1}{n}}$ alle die Werthe $\alpha p^{\frac{1}{n}}, \alpha^2 p^{\frac{1}{n}}, \dots \alpha^{n-1} p^{\frac{1}{n}}$ beilegt.

Man sieht leicht, daß alle diese Werthe von y von einander verschieden sein müssen; denn sonst würde man eine Gleichung von derselben Gestalt wie (3) erhalten, und eine solche Gleichung würde, wie wir sahen, auf Widersprüche führen.

Bezeichnet man also durch $y_1, y_2 \dots y_n$ n verschiedene Wurzeln der Gleichung (1), so findet man

$$y_1 = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} \dots + q_{n-1} p^{\frac{n-1}{n}} \\ y_2 = q_0 + \alpha p^{\frac{1}{n}} + \alpha^2 q_2 p^{\frac{2}{n}} \dots + \alpha^{n-1} q_{n-1} p^{\frac{n-1}{n}} \\ \dots \\ y_n = q_0 + \alpha^{n-1} p^{\frac{1}{n}} + \alpha^{n-2} q_2 p^{\frac{2}{n}} \dots + \alpha q_{n-1} p^{\frac{n-1}{n}}.$$

Aus diesen n Gleichungen folgt leicht

$$q_0 = \frac{1}{n}(y_1 + y_2 \dots + y_n) \\ p^{\frac{1}{n}} = \frac{1}{n}(y_1 + \alpha^{n-1} y_2 + \alpha^{n-2} y_3 \dots + \alpha y_n) \\ q_2 p^{\frac{2}{n}} = \frac{1}{n}(y_1 + \alpha^{n-2} y_2 + \alpha^{n-4} y_3 \dots + \alpha^2 y_n) \\ \dots$$

$$q_{n-1}p^{\frac{n-1}{n}} = \frac{1}{n}(y_1 + \alpha y_2 + \alpha^2 y_3 \dots + \alpha^{n-1} y_n).$$

Man sieht daraus, daß alle die Größen $p^{\frac{1}{n}}, q_0, q_2 \dots q_{n-1}$ durch rationale Functionen der gegebenen Gleichung ausgedrückt werden können.

In der That ist

$$q_\mu = n^{\mu-1} \cdot \frac{y_1 + \alpha^{-\mu} y_2 + \alpha^{-2\mu} y_3 \dots + \alpha^{-(n-1)\mu} y_n}{(y_1 + \alpha^{-1} y_2 + \alpha^{-2} y_3 \dots + \alpha^{-(n-1)} y_n)^\mu}$$

Man nehme nun eine allgemeine Gleichung vom Grade m an, z. B.

$$0 = a_0 + a_1 x + a_2 x^2 \dots + a_{m-1} x^{m-1} + x^m$$

und setze, sie sei algebraisch auflösbar. Es sei

$$x = s_0 + \varrho^{\frac{1}{n}} + s_2 \varrho^{\frac{2}{n}} \dots + s_{n-1} \varrho^{\frac{n-1}{n}},$$

so lassen sich dem Obigen zu Folge die Größen ϱ, s_0, s_2 etc. durch rationale Functionen von $x_1, x_2 \dots x_m$ ausdrücken, wenn man durch $x_1, x_2 \dots x_m$ die Wurzeln der gegebenen Gleichung bezeichnet.

Nun untersuche man irgend eine der Größen ϱ, s_0, s_2 etc., zum Beispiel ϱ . Man bezeichne durch $\varrho, \varrho_2, \dots \varrho_n$, die verschiedenen Werthe von ϱ , welche man findet, wenn man die Wurzeln $x_1, x_2 \dots x_m$ auf alle mögliche Weise untereinander verwechselt; so läßt sich eine Gleichung vom Grade n' aufstellen, deren Coefficienten rationale Functionen von $a_0, a_1, \dots a_{n-1}$ und deren Wurzeln die Größen $\varrho_1, \varrho_2 \dots \varrho_{n'}$ sind, welche rationale Functionen der Größen $x_1, x_2 \dots x_m$ sind. Setzt man also

$$\varrho = t_0 + u^{\frac{1}{\nu}} + t_2 u^{\frac{2}{\nu}} \dots + t_{\nu-1} u^{\frac{\nu-1}{\nu}}$$

so sind alle die Größen $u^{\frac{1}{\nu}}, t_0, t_2 \dots t_{\nu-1}$ rationale Functionen von $\varrho_1, \varrho_2, \dots \varrho_{n'}$, also auch von $x_1, x_2 \dots x_m$. Verfährt man eben so mit den Größen u, t_0, t_2 etc., so folgt Nachstehendes:

Wenn eine Gleichung algebraisch auflösbar ist, so kann man der Wurzel allezeit eine solche Form geben, daß sich alle algebraische Functionen, aus welchen sie zusammengesetzt ist, durch rationale Functionen der Wurzeln der gegebenen Gleichung ausdrücken lassen.

§. III. Ueber die Zahl der verschiedenen Werthe, welche eine Function mehrerer Größen haben kann, wenn man die Größen, von welchen sie abhängt, unter einander vertauscht.

Es sei v eine rationale Function mehrerer von einander unabhängiger Größen $x_1, x_2 \dots x_n$. Die Zahl der verschiedenen Werthe, deren diese Func-

tion durch Vertauschung der Größen, von welchen sie abhängt, fähig ist, kann nicht größer sein als das Product $1 \cdot 2 \cdot 3 \dots n$. Dieses Product sei gleich μ . Nun sei

$$v \begin{pmatrix} \alpha & \beta & \gamma & \delta & \dots \\ a & b & c & d & \dots \end{pmatrix}$$

der Werth, welchen eine beliebige Function v bekommt, wenn man darin x_a, x_b, x_c, x_d etc. statt $x_\alpha, x_\beta, x_\gamma, x_\delta$ etc. setzt, so ist klar, daß wenn man durch $A_1, A_2 \dots A_\mu$ die verschiedenen Formen bezeichnet, deren $1, 2, 3, 4 \dots n$ durch Verwechselung der Zeiger $1, 2, 3 \dots n$ fähig ist, die verschiedenen Werthe von v durch

$$v \begin{pmatrix} A_1 \\ A_1 \end{pmatrix}, v \begin{pmatrix} A_1 \\ A_2 \end{pmatrix}, v \begin{pmatrix} A_1 \\ A_3 \end{pmatrix} \dots v \begin{pmatrix} A_1 \\ A_\mu \end{pmatrix}$$

ausgedrückt werden können. Man setze, die Zahl der verschiedenen Werthe welche v hat sei kleiner als μ , so müssen mehrere Werthe von v *einander gleich* sein. Es sei also

$$v \begin{pmatrix} A_1 \\ A_1 \end{pmatrix} = v \begin{pmatrix} A_1 \\ A_2 \end{pmatrix} \dots = v \begin{pmatrix} A_1 \\ A_m \end{pmatrix}.$$

Unterwirft man diese Größen der durch $\begin{pmatrix} A_1 \\ A_{m+1} \end{pmatrix}$ bezeichneten Verwandlung, so bekommt man die neue Reihe gleicher Werthe:

$$v \begin{pmatrix} A_1 \\ A_{m+1} \end{pmatrix} = v \begin{pmatrix} A_1 \\ A_{m+2} \end{pmatrix} \dots = v \begin{pmatrix} A_1 \\ A_{2m} \end{pmatrix},$$

welche Größen von den vorigen verschieden, aber an Zahl ihnen gleich sind. Verwandelt man diese Größen von Neuem, wie es durch $\begin{pmatrix} A_1 \\ A_{2m+1} \end{pmatrix}$ ausgedrückt wird, so erhält man ein neues System von gleichen Größen, die sämmtlich von den vorigen verschieden sind. Führt man auf diese Weise fort, bis die möglichen Verwandlungen erschöpft sind, so werden die μ Werthe von v in eine gewisse Zahl von Systemen, jedes von m gleichen Werthen, zerlegt sein. Es folgt also, daß wenn die Zahl der verschiedenen Werthe von v gleich ϱ ist, welche Zahl der Zahl der Systeme gleich kommt, daß dann

$$\varrho m = 2 \cdot 3 \cdot 4 \dots n$$

sein muß, das heißt:

Die Zahl der verschiedenen Werthe, welche eine Function von n Größen durch die möglichen Vertauschungen dieser Größen erhalten kann, ist nothwendig ein Submultiplum des Products $1 \cdot 2 \cdot 3 \dots n$; wie bekannt.

Es sei nunmehr $\begin{pmatrix} A_1 \\ A_m \end{pmatrix}$ eine beliebige Verwandlung. Dieselbe werde mit v mehreremal vorgenommen, so entsteht eine Reihe von Werthen

$$v, v_1, v_2 \dots v_{p-1}, v_p,$$

und es ist klar, daß v nothwendig wiederholt vorkommen muß. Kehrt v nach p Verwandlungen wieder, so nennt man $\begin{pmatrix} A_1 \\ A_m \end{pmatrix}$ *wiederkehrende Verwandlung von der p^{ten} Ordnung*. Man hat alsdann die periodische Reihe

$$v, v_1, v_2 \dots v_{p-1}, v, v_1, v_2 \dots,$$

oder wenn man durch $v\left(\frac{A_1}{A_m}\right)^r$ den Werth von v bezeichnet, welcher entsteht, nachdem die durch $\left(\frac{A_1}{A_m}\right)$ bezeichnete Verwandlung r mal wiederholt worden, die Reihe

$$v\left(\frac{A_1}{A_m}\right)^0, v\left(\frac{A_1}{A_m}\right)^1, v\left(\frac{A_1}{A_m}\right)^2 \dots v\left(\frac{A_1}{A_m}\right)^{p-1}, v\left(\frac{A_1}{A_m}\right)^0 \dots$$

Hieraus folgt, daß

$$\begin{aligned} v\left(\frac{A_1}{A_m}\right)^{\alpha p+r} &= v\left(\frac{A_1}{A_m}\right)^r \\ v\left(\frac{A_1}{A_m}\right)^{\alpha p} &= v\left(\frac{A_1}{A_m}\right)^0 = v. \end{aligned}$$

Nun setze man, p sei die größte in n enthaltene Primzahl, und die Zahl der verschiedenen Werthe von v sei kleiner als p , so müssen unter p beliebigen Werthen von v nothwendig zwei einander gleich sein.

Es müssen also zwei von den p Werthen

$$v\left(\frac{A_1}{A_m}\right)^0, v\left(\frac{A_1}{A_m}\right)^1, v\left(\frac{A_1}{A_m}\right)^2 \dots v\left(\frac{A_1}{A_m}\right)^{p-1}$$

gleich sein. Es sei z. B.

$$v\left(\frac{A_1}{A_m}\right)^r = v\left(\frac{A_1}{A_m}\right)^{r'},$$

so folgt daraus

$$v\left(\frac{A_1}{A_m}\right)^{r+p-r} = v\left(\frac{A_1}{A_m}\right)^{r'+p-r}$$

Dieses giebt, weil $v\left(\frac{A_1}{A_m}\right)^p = v$, wenn man r statt $r' + p - r$ setzt,

$$v = v\left(\frac{A_1}{A_m}\right)^r;$$

wo r offenbar kein Vielfaches von p ist. Der Werth von v wird also durch die Substitution $\left(\frac{A_1}{A_m}\right)^r$ nicht mehr verwandelt, folglich auch nicht durch die Wiederholung derselben. Es ist also

$$v = v\left(\frac{A_1}{A_m}\right)^{r\alpha},$$

wo α eine ganze Zahl bedeutet.

Wenn nun p eine Primzahl ist, so läßt sich offenbar immer eine ganze Zahl β finden, von der Art, daß

$$r\alpha = p\beta + 1.$$

Also ist

$$v = v\left(\frac{A_1}{A_m}\right)^{p\beta+1},$$

oder weil $v = v \binom{A_1}{A_m}^{p\beta}$ war,

$$v = v \binom{A_1}{A_m}.$$

Der Werth von v wird also durch die *wiederkehrende* Verwandlung $\binom{A_1}{A_m}$ vom Grade p nicht verändert.

Nun ist klar, daß

$$\begin{pmatrix} \alpha & \beta & \gamma & \delta & \dots & \zeta & \eta \\ \beta & \gamma & \delta & \varepsilon & \dots & \eta & \alpha \end{pmatrix} \text{ und } \begin{pmatrix} \beta & \gamma & \delta & \varepsilon & \dots & \eta & \alpha \\ \gamma & \alpha & \beta & \delta & \dots & \zeta & \eta \end{pmatrix}$$

zwei *wiederkehrende* Verwandlungen vom Grade p sind, wenn die Zahl der Zeiger $\alpha, \beta, \gamma, \dots, \eta$ gleich p ist. Der Werth von v wird also auch durch die Verbindung dieser beiden Verwandlungen nicht verändert. Die beiden Verwandlungen sind aber offenbar gleich bedeutend mit der einen

$$\begin{pmatrix} \alpha & \beta & \gamma \\ \gamma & \alpha & \beta \end{pmatrix}$$

und diese eine mit den beiden nach einander vorgenommenen

$$\begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix} \text{ und } \begin{pmatrix} \beta & \gamma \\ \gamma & \beta \end{pmatrix}.$$

Der Werth von v wird also durch diese beiden mit einander verbundenen Verwandlungen nicht verändert. Also ist

$$v = v \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix} \begin{pmatrix} \beta & \gamma \\ \gamma & \beta \end{pmatrix}$$

und eben so

$$v = v \begin{pmatrix} \beta & \gamma \\ \gamma & \beta \end{pmatrix} \begin{pmatrix} \gamma & \delta \\ \delta & \gamma \end{pmatrix},$$

woraus

$$v = v \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix} \begin{pmatrix} \gamma & \delta \\ \delta & \gamma \end{pmatrix}$$

folgt.

Man sieht hieraus, daß die Function v durch zwei aufeinander folgende Verwandlungen von der Form $\begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix}$, wenn α und β zwei beliebige Zeiger sind, nicht verändert wird. Nennt man daher eine solche Verwandlung, *Versetzung* (Transposition), so folgt, daß ein beliebiger Werth von v durch eine grade Zahl von Versetzungen nicht verändert wird, und daß folglich alle Werthe von v , welche eine ungrade Zahl von Versetzungen geben, gleich sind. Jede beliebige Vertauschung der Elemente einer Function kann aber durch eine gewisse Zahl von Versetzungen geschehen: Die Function v kann also nicht mehr als zwei verschiedene Werthe haben. Dieses giebt folgenden Lehrsatz:

Die Zahl der verschiedenen Werthe einer Function von n Größen kann entweder gar nicht bis unter die größte Primzahl, die sich unter den Factoren von n befindet, vermindert werden, oder nur bis auf 2 oder 1.

Es ist also unmöglich, eine Function von fünf Größen zu finden, welche 3 oder 4 verschiedene Werthe hätte.

Der Beweis dieses Lehrsatzes ist aus einem Mémoire von *Cauchy* genommen, welches sich in dem 17ten Hefte des *Journal de l'école polytechnique* pag. 1 etc. befindet.

Es mögen nun v und v' zwei Functionen sein, welche jede zwei verschiedene Werthe haben, so ist dem Vorigen zufolge klar, daß wenn man durch v_1, v_2 und v'_1, v'_2 jene doppelten Werthe bezeichnet, daß alsdann die beiden Ausdrücke

$$v_1 + v_2 \text{ und } v_1 v'_1 + v_2 v'_2$$

symmetrische Functionen sind. Es sei

$$v_1 + v_2 = t \text{ und } v_1 v'_1 + v_2 v'_2 = t_1,$$

so findet man

$$v_1 = \frac{t \cdot v'_2 - t_1}{v'_2 - v'_1}.$$

Man setze nunmehr die Zahl der Größen $x_1, x_2 \dots x_m$ sei fünf, so ist das Product

$$\varrho = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_1 - x_5)(x_2 - x_3)(x_2 - x_4)(x_2 - x_5)(x_3 - x_4)(x_3 - x_5)(x_4 - x_5)$$

offenbar eine Function, welche zwei verschiedene Werthe hat; der zweite

Werth ist die nemliche Function mit entgegengesetztem Zeichen. Setzt man also $v'_1 = \varrho$, so ist $v'_2 = -\varrho$. Der Ausdruck von v_1 ist also

$$v_1 = \frac{t_1 + \varrho t_2}{2\varrho}, \text{ oder}$$

$$v_1 = \frac{1}{2}t_2 + \frac{t_1}{2\varrho^2}\varrho,$$

wo $\frac{1}{2}t_2$ eine symmetrische Function ist. ϱ hat zwei Werthe, die nur dem Zeichen nach verschieden sind, so daß also $\frac{t_1}{2\varrho^2}$ ebenfalls eine symmetrische Function ist.

Setzt man also $\frac{1}{2}t_2 = p$ und $\frac{t_1}{2\varrho^2} = q$, so folgt

daß jede Function von fünf Größen, welche zwei verschiedene Werthe hat, durch $p + q \cdot \varrho$ ausgedrückt werden kann, wo p und q zwei symmetrische Functionen sind und

$$\varrho = (x_1 - x_2)(x_1 - x_3) \dots (x_4 - x_5)$$

ist.

Für unsern Zweck ist noch die allgemeine Form der Functionen von fünf Größen nöthig, welche fünf verschiedene Werthe haben. Man kann dieselben, wie folgt, finden.

Es sei v eine rationale Function der Größen x_1, x_2, x_3, x_4, x_5 , welche die Eigenschaft hat, unveränderlich zu sein, wenn man beliebige vier von den fünf Größen z. B. x_2, x_3, x_4, x_5 untereinander vertauscht. Unter dieser Bedingung ist

v offenbar nach x_2, x_3, x_4, x_5 symmetrisch. Man kann also v durch eine rationale Function von x_1 und symmetrische Functionen von x_2, x_3, x_4, x_5 ausdrücken. Jede symmetrische Function dieser Größe kann aber durch eine rationale Function der Coefficienten einer Gleichung vom vierten Grade ausgedrückt werden, deren Wurzeln x_2, x_3, x_4, x_5 sind. Setzt man also

$$(x - x_2)(x - x_3)(x - x_4)(x - x_5) = x^4 - px^3 + qx^2 - rx + s,$$

so kann die Function v durch eine rationale Function von x_1, p, q, r, s ausgedrückt werden. Setzt man aber

$$(x - x_1)(x - x_2)(x - x_3)(x - x_4)(x - x_5) = x^5 - ax^4 + bx^3 - cx^2 + dx - e,$$

so erhält man

$$\begin{aligned} (x - x_1)(x^4 - px^3 + qx^2 - rx + s) &= x^5 - ax^4 + bx^3 - cx^2 + dx - e \\ &= x^5 - (p + x_1)x^4 + (q + px_1)x^3 - (r + qx_1)x^2 + (s + rx_1)x - sx_1, \end{aligned}$$

woraus

$$p = a - x_1$$

$$q = b - ax_1 + x_1^2$$

$$r = c - bx_1 + ax_1^2 - x_1^3$$

$$s = d - cx_1 + bx_1^2 - ax_1^3 + x_1^4$$

folgt. Es läßt sich also v durch eine rationale Function von x_1, a, b, c, d und e ausdrücken.

Daraus folgt, daß man v auf folgende Gestalt bringen kann:

$$v = \frac{t}{\varphi(x_1)}$$

wo t und $\varphi(x_1)$ zwei ganze Functionen von x_1, a, b, c, d und e sind. Multiplicirt man diesen Bruch oben und unten mit $\varphi(x_2), \varphi(x_3), \varphi(x_4), \varphi(x_5)$, so findet man

$$v = \frac{t \cdot \varphi(x_2) \cdot \varphi(x_3) \cdot \varphi(x_4) \cdot \varphi(x_5)}{\varphi(x_1) \cdot \varphi(x_2) \cdot \varphi(x_3) \cdot \varphi(x_4) \cdot \varphi(x_5)}.$$

Nun ist $\varphi(x_2) \cdot \varphi(x_3) \cdot \varphi(x_4) \cdot \varphi(x_5)$, wie man sieht, eine ganze und symmetrische Function von x_2, x_3, x_4, x_5 . Man kann also dieses Product durch eine ganze Function von p, q, r, s ausdrücken, also auch durch eine ganze Function von x_1, a, b, c, d . Der Zähler des obigen Bruchs ist also eine ganze Function der nemlichen Größe; der Nenner ist eine symmetrische Function von x_1, x_2, x_3, x_4, x_5 und kann also durch eine rationale Function von a, b, c, d, e ausgedrückt werden. Daraus folgt, daß man

$$v = r_0 + r_1x_1 + r_2x_1^2 \dots + r_mx_1^m$$

setzen kann. Multiplicirt man die Gleichung

$$x_1^5 = ax_1^4 - bx_1^3 + cx_1^2 - dx_1 + e$$

mit $x_1, x_1^2 \dots x_1^{m-5}$, so ist klar, daß man $m - 4$ Gleichungen erhält, aus welchen sich der Reihe nach $x_1^5, x_1^6 \dots x_1^m$ finden lassen, und zwar durch Größen von der Form

$$\alpha + \beta x_1 + \gamma x_1^2 + \delta x_1^3 - \varepsilon x_1^4,$$

in welchen $\alpha, \beta, \gamma, \delta, \varepsilon$ rationale Functionen von a, b, c, d, e sind.

Man kann also v auf die Form

$$v = r_0 + r_1 x_1 + r_2 x_1^2 + r_3 x_1^3 + r_4 x_1^4 \quad (a)$$

bringen, wo r_0, r_1, r_2 etc. rationale Functionen von a, b, c, d, e sind, das heißt symmetrische Functionen von x_1, x_2, x_3, x_4, x_5 .

Dieses ist die allgemeine Form der Functionen, welche sich nicht verändern, wenn man die Größen x_2, x_3, x_4, x_5 vertauscht. Sie haben entweder fünf verschiedene Werthe, oder sie sind symmetrisch.

Es sei nunmehr v irgend eine rationale Function von x_1, x_2, x_3, x_4, x_5 , welche die fünf Werthe v_1, v_2, v_3, v_4, v_5 hat. Man nehme die Function $x_1^m v$:

Verwechselt man in derselben die vier Größen x_2, x_3, x_4, x_5 auf alle mögliche Art, so wird $x_1^m v$ jedesmal einen der Werthe

$$x_1^m v_1, x_1^m v_2, x_1^m v_3, x_1^m v_4, x_1^m v_5$$

bekommen.

Nun behaupte ich, daß die Zahl der durch diese Vertauschung entstehenden Werthe von $x_1^m v$ *kleiner als fünf ist*. Denn nimmt man alle fünf Werthe an, so entstehen durch die Vertauschung von x_1 mit x_2, x_3, x_4, x_5 aus diesen Werthen *zwanzig* andere, die nothwendig unter sich und von den vorigen verschieden sind. Die Function würde also überhaupt 25 verschiedene Werthe haben, welches nicht möglich ist; denn 25 ist kein Divisor des Products $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$. Bezeichnet man also durch μ die Zahl der Werthe, welche v bekommt, wenn man die Größen x_2, x_3, x_4, x_5 unter einander vertauscht, so muß μ einen der vier Werthe 1, 2, 3, 4 haben.

1. Es sei $\mu = 1$, so ist v , vermöge des Obigen, von der Form (a).

2. Es sei $\mu = 4$, so ist $v_1 + v_2 + v_3 + v_4$ eine Function von der Form (a). Es ist aber

$$v_5 = (v_1 + v_2 + v_3 + v_4 + v_5) - (v_1 + v_2 + v_3 + v_4)$$

= einer *symmetrischen* Function, weniger $(v_1 + v_2 + v_3 + v_4)$; also ist v_5 von der Form (a).

3. Es sei $\mu = 2$, so ist $v_1 + v_2$ eine Function von der Form (a). Es sei also

$$v_1 + v_2 = r_0 + r_1 x_1 + r_2 x_1^2 + r_3 x_1^3 + r_4 x_1^4 = \varphi(x_1)$$

Vertauscht man der Reihe nach x_1 mit x_2, x_3, x_4, x_5 , so erhält man

$$v_1 + v_2 = \varphi(x_1)$$

$$v_2 + v_3 = \varphi(x_2)$$

...

$$v_{m-1} + v_m = \varphi(x_{m-1})$$

$$v_m + v_1 = \varphi(x_m),$$

wo m eine der Zahlen 2, 3, 4, 5 ist. Für $m = 2$ ist $\varphi(x_1) = \varphi(x_2)$, welches nicht möglich ist, weil die Zahl der Werthe von $\varphi(x_1)$ *fünf* sein soll. Für $m = 3$ ist

$$v_1 + v_2 = \varphi(x_1), \quad v_2 + v_3 = \varphi(x_2), \quad v_3 + v_1 = \varphi(x_3),$$

welches

$$2v_1 = \varphi(x_1) - \varphi(x_2) + \varphi(x_3)$$

gibt. Das zweite Glied dieser Gleichung hat aber mehr als fünf Werthe, nemlich 30. Auf dieselbe Weise läßt sich zeigen, daß auch m nicht gleich 4 sein kann. μ kann also nicht gleich zwei sein.

4. Es sei $\mu = 3$. Alsdann hat $v_1 + v_2 + v_3$, folglich auch $v_4 + v_5 = (v_1 + v_2 + v_3 + v_4 + v_5) - (v_1 + v_2 + v_3)$, fünf Werthe. Wir sahen aber, daß diese Voraussetzung nicht Statt findet. Also kann auch nicht $\mu = 3$ sein.

Zusammengenommen also findet man folgenden Lehrsatz:

Jede rationale Function von fünf Größen, welche fünf verschiedene Werthe hat, ist nothwendig von der Form

$$r_0 + r_1x + r_2x^2 + r_3x^3 + r_4x^4,$$

wo r_0, r_1, r_2 etc. symmetrische Functionen sind, und x eine von den fünf Größen ist.

Aus

$$r_0 + r_1x + r_2x^2 + r_3x^3 + r_4x^4 = v$$

findet man leicht, wenn man von der gegebenen Gleichung Gebrauch macht, den Werth von x , wie folgt, ausgedrückt

$$x = s_0 + s_1v + s_2v^2 + s_3v^3 + s_4v^4$$

wo s_0, s_1, s_2 etc. eben wie r_0, r_1, r_2 , etc., symmetrische Functionen sind.

Es sei v irgend eine rationale Function, welche m verschiedene Werthe $v_1, v_2, v_3 \dots v_m$ hat. Setzt man

$$(v - v_1)(v - v_2)(v - v_3) \dots (v - v_m) = q_0 + q_1v + q_2v^2 \dots + q_{m-1}v^{m-1} + v^m = 0,$$

so sind bekanntlich $q_0, q_1, q_2 \dots$ symmetrische Functionen, und die m Wurzeln der Gleichung sind $v_1, v_2 \dots v_m$. Nun behaupte ich, daß es unmöglich ist, den Werth von v als Wurzel einer Gleichung von derselben Form, aber von einem niedrigeren Grade auszudrücken. Denn es sei

$$t_0 + t_1v + t_2v^2 \dots + t_{\mu-1}v^{\mu-1} + v^\mu = 0$$

eine solche Gleichung, wo t_0, t_1 etc. symmetrische Functionen sind, und v_1 sei ein Werth von v , der der Gleichung genug thut, so ist

$$v^\mu + t_{\mu-1}v^{\mu-1} \dots = (v - v_1) \cdot P_1.$$

Verwechselt man nun unter einander die Elemente der Function, so findet man folgende Reihe von Gleichungen:

$$v^\mu + t_{\mu-1}v^{\mu-1} \dots = (v - v_2) \cdot P_2,$$

$$v^\mu + t_{\mu-1}v^{\mu-1} \dots = (v - v_3) \cdot P_3,$$

...

$$v^\mu + t_{\mu-1}v^{\mu-1} \dots = (v - v_m) \cdot P_m.$$

Daraus folgt, daß $v - v_1, v - v_2, v - v_3 \dots v - v_m$ sämmtlich Factoren von $v^\mu + t_{\mu-1}v^{\mu-1} \dots$ sind, und daß folglich μ nothwendig gleich m sein muß. Man erhält daher folgenden Lehrsatz:

Wenn eine rationale Function mehrerer Größen m verschiedene Werthe hat, so läßt sich allezeit eine Gleichung vom Grade m finden, deren Coefficienten symmetrische Functionen sind, und welche jene Werthe zu Wurzeln haben; aber es ist nicht möglich eine Gleichung von der nämlichen Form von niedrigerem Grade aufzustellen, welche einen oder mehrere jener Werthe zu Wurzeln hat.

§. IV. Beweis der Unmöglichkeit der allgemeinen Auflösung der Gleichungen vom fünften Grade.

Vermöge der oben gefundenen Sätze zusammengekommen läßt sich behaupten: daß es unmöglich ist, Gleichungen vom fünften Grade allgemein aufzulösen.

Nach (§. II.) nämlich können alle algebraische Functionen, aus welchen ein algebraischer Ausdruck der Wurzeln zusammengesetzt sein mag, durch rationale Functionen der Wurzeln der Gleichung ausgedrückt werden.

Da es nun unmöglich ist, die Wurzel einer Gleichung allgemein durch eine rationale Function der Coefficienten auszudrücken, so muß

$$R^{\frac{1}{m}} = v \dots$$

sein, wo m eine Primzahl und R eine rationale Function der Coefficienten der gegebenen Gleichung, das heißt, eine symmetrische Function der Wurzeln ist; v ist eine rationale Function der Wurzeln. Daraus folgt:

$$v^m - R = 0$$

und da es zufolge (§. II.) unmöglich ist, den Grad dieser Gleichung zu erniedrigen, so wird die Function v , zufolge des letzten Lehrsatzes im vorigen Paragraph, m verschiedene Werthe haben. Da nun m ein Divisor von $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$ sein muß, so kann m gleich 2, 3 oder 5 sein. Nun existirt aber zufolge (§. III.) keine

Function von fünf Größen, welche 3 Werthe hat: es muß also $m = 5$ oder $m = 2$ sein. Es sei $m = 5$; so erhält man, zufolge des vorigen Paragraphs,

$$\sqrt[5]{R} = r_0 + r_1x + r_2x^2 + r_3x^3 + r_4x^4$$

und hieraus

$$x = s_0 + s_1R^{\frac{1}{5}} + s_2R^{\frac{2}{5}} + s_3R^{\frac{3}{5}} + s_4R^{\frac{4}{5}}.$$

Nach (§. II.) folgt daraus

$$s_1R^{\frac{1}{5}} = x_1 + \alpha^4x_2 + \alpha^3x_3 + \alpha^2x_4 + \alpha x_5,$$

wo $\alpha^5 = 1$. Diese Gleichung ist unmöglich, weil das zweite Glied 120 Werthe hat, und gleichwohl die Wurzel einer Gleichung vom fünften Grade $z^5 - s_1^5R = 0$ ist.

Es muß also $m = 2$ sein.

Alsdann ist nach (§. II.)

$$\sqrt{R} = p + qs,$$

wo p und q symmetrische Functionen sind, und

$$s = (x_1 - x_2) \dots (x_4 - x_5)$$

ist. Also ist, wenn man x_1 mit x_2 vertauscht,

$$-\sqrt{R} = p - qs,$$

woraus $p = 0$ und $\sqrt{R} = qs$ folgt. Man sieht daraus, daß alle algebraische Functionen vom ersten Grade, welche sich in dem Ausdruck der Wurzeln befinden, von der Form $\alpha + \beta \cdot \sqrt{s^2} = \alpha + \beta s$ sein müssen, wo α und β symmetrische Functionen sind. Da es nun unmöglich ist, die Wurzeln durch eine Function von der Form $\alpha + \beta\sqrt{R}$ auszudrücken, so muß eine Gleichung von der Form

$$\sqrt[m]{(\alpha + \beta\sqrt{s^2})} = v$$

Statt finden, wo α und β nicht gleich Null sind, m eine Primzahl ist, α und β symmetrische Functionen sind, und v eine rationale Function der Wurzeln ist. Dieses giebt

$$\sqrt[m]{(\alpha + \beta s)} = v_1 \text{ und } \sqrt[m]{(\alpha - \beta s)} = v_2,$$

wo v_1 und v_2 rationale Functionen sind. Multiplicirt man v_2 mit v_1 , so erhält man

$$v_2v_1 = \sqrt[m]{(\alpha^2 - \beta^2s^2)}.$$

Nun ist $\alpha^2 - \beta^2s^2$ eine symmetrische Function. Wenn also $\sqrt[m]{(\alpha^2 - \beta^2s^2)}$ nicht eine symmetrische Function wäre, so müßte, dem Obigen zufolge, $m = 2$ sein. Alsdann aber ist $v = \sqrt{(\alpha + \beta\sqrt{s^2})}$, und v hat folglich vier verschiedene Werthe;

welches nicht möglich ist. Es muß also $\sqrt[m]{(\alpha^2 - \beta^2 s^2)}$ eine symmetrische Function sein. Eine solche Function sei γ , so ist

$$v_2 v_1 = \gamma \text{ und } v_2 = \frac{\gamma}{v_1}.$$

Nun nehme man den Ausdruck

$$\begin{aligned} v_1 + v_2 &= \sqrt[m]{(\alpha + \beta\sqrt{s^2})} + \frac{\gamma}{\sqrt[m]{(\alpha + \beta\sqrt{s^2})}} = p \\ &= \sqrt[m]{R} + \frac{\gamma}{\sqrt[m]{R}} = R^{\frac{1}{m}} + \frac{\gamma}{R} R^{\frac{m-1}{m}}. \end{aligned}$$

Man bezeichne die Werthe, welche p bekommen kann, wenn man $\alpha R^{\frac{1}{m}}, \alpha^2 R^{\frac{1}{m}}, \alpha^3 R^{\frac{1}{m}} \dots \alpha^{m-1} R^{\frac{1}{m}}$ statt $R^{\frac{1}{m}}$ setzt, wo

$$\alpha^{m-1} + \alpha^{m-2} \dots + \alpha + 1 = 0$$

ist, durch $p_1, p_2 \dots p_m$, und mache das Product

$$(p - p_1)(p - p_2) \dots (p - p_m) = p^m - A p^{m-1} + A_1 p^{m-2} \dots = 0,$$

so ist leicht zu sehen, daß A, A_1 etc. rationale Functionen der Coefficienten der gegebenen Gleichung, also symmetrische Functionen der Wurzeln sein werden. Diese Gleichung ist aber offenbar irreductibel. Also muß p , zufolge des letzten Lehrsatzes im vorigen Paragraph, als Function der Wurzeln betrachtet, m verschiedene Werthe haben. Folglich ist $m = 5$. Alsdann aber ist p von der Form (a) im vorigen Paragraph. Also wird

$$\sqrt[5]{R} + \frac{\gamma}{\sqrt[5]{R}} = r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4 = p,$$

folglich

$$x = s_0 + s_1 p + s_2 p^2 + s_3 p^3 + s_4 p^4,$$

das heißt, es wird, wenn man $R^{\frac{1}{5}} + \frac{\gamma}{R} R^{\frac{4}{5}}$ statt p setzt,

$$x = t_0 + t_1 R^{\frac{1}{5}} + t_2 R^{\frac{2}{5}} + t_3 R^{\frac{3}{5}} + t_4 R^{\frac{4}{5}}$$

sein, wo t_0, t_1, t_2 etc. rationale Functionen von R und von den Coefficienten der gegebenen Gleichung sind. Daraus folgt, vermöge (§. II.)

$$t_1 R^{\frac{1}{5}} = x_1 + \alpha^4 x_2 + \alpha^3 x_3 + \alpha^2 x_4 + \alpha x_5 = p,$$

wo

$$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$$

ist. Aus $p = t_1 R^{\frac{1}{5}}$ folgt aber $p^5 = t_1^5 R$, und weil $t_1^5 R$ von der Form $u + u_1 \sqrt{s^2}$ ist, $p^5 = u + u_1 \sqrt{s^2}$, welches

$$(p^5 - u)^2 = u_1^2 s^2$$

giebt. Diese Gleichung giebt, wie man sieht, p durch eine Gleichung vom 10^{ten} Grade, deren Coefficienten sämmtlich symmetrische Functionen sind, welches aber, zufolge des letzten Lehrsatzes im vorigen Paragraph, nicht möglich ist; denn da³

$$p = x_1 + \alpha^4 x_2 + \alpha^3 x_3 + \alpha^4 x_4 + \alpha x_5$$

ist, so würde p , 120 verschiedene Werthe haben; welches ein Widerspruch ist.

Wir schließen aus diesem Allen:

daß es unmöglich ist, Gleichungen vom fünften Grade allgemein algebraisch aufzulösen.

Daraus folgt unmittelbar weiter, daß es ebenfalls unmöglich ist, Gleichungen von höheren als dem fünften Grade allgemein aufzulösen. Mithin sind die Gleichungen, welche sich algebraisch allgemein auflösen lassen, nur die von den vier ersten Graden.

³*Editorial note:* In this last occurrence the coefficient of x_4 is printed α^4 ; the identical resolvent above and on p. 82 has $\alpha^2 x_4$. An apparent misprint for $\alpha^2 x_4$, reproduced here as printed.