Werk

Titel: Beweis der Unmöglichkeit, algebraische Gleichungen von höheren Graden als dem vie...

Autor: Abel, N.H.

Jahr: 1826

PURL: https://resolver.sub.uni-goettingen.de/purl?243919689_0001|log12

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

8.

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 heifst nichts anders, als ihre Wurzeln durch eine algebraische Function der Coefficienten ausdrücken. Man mufs also erst die allgemeine Form algebraischer Functionen betrachten und alsdann untersuchen, ob es möglich sei, der gegebenen Gleichung auf die Weise genug zu thun, dafs man den Ausdruck einer algebraischen Function statt der unbekannten Gröfse setzt.

§. I.

Ueber die allgemeine Form algebraischer Functionen.

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

Läfst sich die Function φ durch die drei ersten der vier obigen Operationen zusammensetzen, so ist sie algebraisch rational oder blos rational; und

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

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

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

ausgedrückt werden kann, wo A eine von x', x'' etc. unabhängige Gröfse ist, und m_1, m_2 etc. ganze positive Zahlen bedeuten; so ist klar, dafs die zwei ersten obigen Operationen besondere Fälle der durch $f(x', x'' \ldots\ldots)$ 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 v', v'', v''' etc. mehrere Functionen der Gröfsen x', x'', $x''' \ldots\ldots$ von der nämlichen Form wie $f(x', x'' \ldots\ldots)$, so ist auch offenbar $f(v', v'', v''' \ldots\ldots)$ eine Function von eben der Form wie $f(x', x'' \ldots\ldots)$. Nun ist $f(v', v'' \ldots\ldots)$ der allgemeine Ausdruck der Functionen, welche durch zweimalige Wiederholung der Operation $f(x', x'' \ldots\ldots)$ entstehen. Man findet also auch immer das nämliche Resultat, wenn man die Operation beliebig oft wiederholt. Daraus folgt, dafs jede ganze Function mehrer Gröfsen x', $x'' \ldots\ldots$ durch die Summe mehrer Glieder von der Form $Ax'^{m_1} x''^{m_2} \ldots\ldots$ ausgedrückt werden kann.

Wir wollen nunmehr die rationalen Functionen betrachten.

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

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

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 v', v'', v''' etc. mehrere Functionen von der Form $\frac{f(x', x'' \ldots)}{\varphi(x', x'' \ldots)}$, so ist leicht zu sehen, dafs $\frac{f(v', v'' \ldots\ldots)}{\varphi(v', v'' \ldots\ldots)}$ wiederum auf die nemliche Form gebracht werden kann. Es folgt also, wie oben bei den ungebrochenen Functionen, dafs jede rationale Function von mehreren Gröfsen x', $x'' \ldots\ldots$ immer auf die Form

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

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

Wir wollen ferner die allgemeine Form algebraischer Functionen suchen.

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

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

die allgemeine Form algebraischer Functionen von x', $x'' \ldots\ldots$ sein, in welchen sich die durch $\sqrt[m]{r}$ 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 Gröfsen von der Form p_1, so wird

$$p_2 = f(x', x'' \ldots\ldots \sqrt[n']{p'}, \sqrt[n'']{p'' \ldots\ldots \sqrt[n_1']{p_1'}, \sqrt[n_1'']{p_1'', \ldots\ldots})$$

die allgemeine Form algebraischer Functionen von x', $x'' \ldots\ldots$ sein, in welchen die Operation $\sqrt[m]{r}$ 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

$$p_3 = f(x', x'' \ldots\ldots \sqrt[n']{p'}, \sqrt[n'']{p'', \ldots\ldots \sqrt[n_1']{p_1'}, \sqrt[n_1'']{p_1'', \ldots \sqrt[n_2']{p_2'} \sqrt[n_2'']{p_2'', \ldots}}),$$

in welchem p_2', p_2'' Functionen der zweiten Ordnung sind, die allgemeine Form algebraischer Functionen von x', $x'' \ldots\ldots$ sein, in welchen die Operation $\sqrt[m]{r}$ sich nur auf rationale und auf algebraische Functionen der ersten und zweiten Ordnung bezieht.

Fährt man auf diese Weise fort, so bekommt man algebraische Functionen von der dritten, vierten .... μ^{ten} Ordnung, und es ist klar, dafs 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 v die Function selbst, so ist

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

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

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

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

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

$$v = f(r', r'', r''' \ldots\ldots\ldots)$$

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

Ist in dem Ausdruck von v die Zahl der Gröfsen $\sqrt[n']{p'}, \sqrt[n'']{p'' \ldots\ldots}$ gleich m, so wollen wir die Function v von der μ^{ten} Ordnung und vom μ^{ten} Grade nennen. Auf diese Weise ist eine Function von der $\overset{m}{\mu}{}^{\text{ten}}$ 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, dafs man setzen kann

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

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

Da eine rationale Function mehrer Gröfsen, wie wir vorhin sahen, immer auf die Form

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

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

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

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

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

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

$$v = \frac{t_0 + t_1 p^{\frac{1}{n}} + t_2 p^{\frac{2}{n}} \ldots\ldots\ldots t_m p^{\frac{m}{n}}}{v_0 + v_1 p^{\frac{1}{n}} + v_2 p^{\frac{2}{n}} \ldots\ldots\ldots v_{m'} p^{\frac{m'}{n}}} = \frac{T}{V}$$

setzen, wo $t_0, t_1 \ldots\ldots t_m$ und $v_0, v_1 \ldots\ldots v_{m'}$ ganze Functionen von r', r'', r''' etc. sind.

Nun mögen $V_1, V_2 \ldots\ldots V_{n-1}$ die $n-1$ Werthe von V sein, welche man findet, wenn man $\alpha . p^{\frac{1}{n}}, \alpha^2 p^{\frac{1}{n}}, \alpha^3 p^{\frac{1}{n}} \ldots\ldots \alpha^{n-1} p^{\frac{1}{n}}$ 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

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

$$v = \frac{T . V_1 . V_2 \ldots\ldots\ldots V_{n-1}}{V . V_1 . V_2 \ldots\ldots\ldots V_{n-1}}.$$

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

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

so findet man

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

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

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

wo $q_0, q_1 \ldots\ldots q_k$ rationale Functionen der Gröfsen p, r', r'' etc. sind.

Welche nun auch die ganze Zahl μ sein mag, so kann man setzen

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

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

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

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

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

wo q_0, q_1, q_2 etc., wie vorhin, rationale Functionen von $p, r', r'' \ldots\ldots$ und

folglich Functionen von der μ^{ten} Ordnung und höchstens vom $m-1^{\text{ten}}$ Grade und von der Art sind, dafs sich $p^{\frac{1}{n}}$ nicht durch rationale Functionen dieser Gröfsen ausdrücken läfst.

In dem ohigen Ausdruck von v kann man immer

$$q_1 = 1$$

setzen. Denn wenn q_1 nicht Null ist, so erhält man, wenn man $p_1 = p.q_1^n$ setzt, $p = \frac{p_1}{q_1^n}$, und $p^{\frac{1}{n}} = \frac{p_1^{\frac{1}{n}}}{q_1}$, also

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

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

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

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

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

haben.

Aus allem diesen folgt Nachstehendes:

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

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

n ist eine Primzahl, $q_0, q_2 \ldots\ldots q_{n-1}$ 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, dafs sich $p^{\frac{1}{n}}$ nicht durch eine rationale Function von $q_0, q_2 \ldots\ldots q_{n-1}$ ausdrücken läfst.

§. II.

Eigenschaften der algebraischen Functionen, welche einer gegebenen Gleichung genugthun.

Es sei

$$c_0 + c_1 y + c_2 y^2 \ldots\ldots + c_{r-1} y^{r-1} + y^r = 0 \quad 1.$$

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

$$y = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} \ldots\ldots + q_{n-1} p^{\frac{n-1}{n}} \quad 2.$$

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

$$r_0 + r_1 p^{\frac{1}{n}} + r_2 p^{\frac{2}{n}} \ldots\ldots + r_{n-1} p^{\frac{n-1}{n}} = 0 \quad 3.$$

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

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

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

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

$$z^n - p = 0 \text{ und}$$
$$r_0 + r_1 z + r_2 z^2 \ldots\ldots + r_{n-1} z^{n-1} = 0$$

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

Die Gleichung sei

$$s_0 + s_1 z + s_2 z^2 \ldots\ldots + s_{k-1} z^{k-1} + z^k = 0$$

und

$$t_0 + t_1 z + t_2 z^2 \ldots\ldots + t_{\mu-1} z^{\mu-1} + z^\mu$$

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

$$t_0 + t_1 z + t_2 z \ldots\ldots + t_{\mu-1} z^{\mu-1} + z^\mu = 0,$$

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

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

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

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

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

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

geben; was nicht sein kann.

Es mufs also

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

sein.

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

Man sieht leicht, dafs 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 $y_1, y_2 \ldots\ldots y_n$ n verschiedene Wurzeln der Gleichung (1), so findet man

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

Aus diesen n Gleichungen folgt leicht

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

Man

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

In der That ist

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

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

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

und setze, sie sei algebraisch auflösbar. Es sei

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

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

Nun untersuche man irgend eine der Gröfsen φ, s_0, s_2 etc., zum Beispiel φ. Man bezeichne durch φ_1, φ_2, ... φ_n, die verschiedenen Werthe von φ, welche man findet, wenn man die Wurzeln x_1, x_2 ..... x_m auf alle mögliche Weise untereinander verwechselt, so läfst sich eine Gleichung vom Grade n' aufstellen, deren Coefficienten rationale Functionen von a_0, a_1, ... a_{n-1} und deren Wurzeln die Gröfsen φ_1, φ_2 ..... $\varphi_{n'}$ sind, welche rationale Functionen der Gröfsen x_1, x_2 ..... x_m sind. Setzt man also

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

so sind alle die Gröfsen $u^{\frac{1}{\nu}}$, t_0, t_2 ..... $t_{\nu-1}$ rationale Functionen von φ_1, φ_2, ... $\varphi_{n'}$, also auch von x_1, x_2, ... x_m. Verfährt man eben so mit den Gröfsen 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, dafs 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 Gröfsen haben kann, wenn man die Gröfsen, von welchen sie abhängt, unter einander vertauscht.

Es sei φ eine rationale Function mehrerer von einander unabhängiger Gröfsen x_1, x_2 ..... x_m. Die Zahl der verschiedenen Werthe, deren diese Fune-

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

$$\varphi\begin{pmatrix}\alpha\beta\gamma\delta\ldots\ldots\\ a\,b\,c\,d\ldots\ldots\end{pmatrix}$$

der Werth, welchen eine beliebige Function φ bekommt, wenn man darin x_a, x_b, x_c x_d etc. statt x_α, x_β, x_γ, x_δ etc. setzt, so ist klar, dafs wenn man durch $A_1, A_2 \ldots . A_\mu$ die verschiedenen Formen bezeichnet, deren $1, 2, 3, 4 \ldots . n$ durch Verwechselung der Zeiger $1, 2, 3 \ldots\ldots n$ fähig ist, die verschiedenen Werthe von φ durch

$$\varphi\begin{pmatrix}A_1\\A_1\end{pmatrix},\quad \varphi\begin{pmatrix}A_1\\A_2\end{pmatrix},\quad \varphi\begin{pmatrix}A_1\\A_3\end{pmatrix}\ldots\ldots\varphi\begin{pmatrix}A_1\\A_\mu\end{pmatrix}$$

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

$$\varphi\begin{pmatrix}A_1\\A_1\end{pmatrix}=\varphi\begin{pmatrix}A_1\\A_2\end{pmatrix}\ldots\ldots=\varphi\begin{pmatrix}A_1\\A_m\end{pmatrix}.$$

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

$$\varphi\begin{pmatrix}A_1\\A_{m+1}\end{pmatrix}=\varphi\begin{pmatrix}A_1\\A_{m+2}\end{pmatrix}\ldots\ldots\ldots=\varphi\begin{pmatrix}A_1\\A_{2m}\end{pmatrix},$$

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

$$\varrho m = 2 . 3 . 4 \ldots\ldots\ldots n$$

sein mufs; das heifst:

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

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

$$\varphi,\ \varphi_1,\ \varphi_2 \ldots\ldots\ldots \varphi_{p-1},\ \varphi_p,$$

und es ist klar, dafs φ nothwendig wiederholt vorkommen mufs. Kehrt φ 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

$$\varphi,\ \varphi_1,\ \varphi_2 \ldots\ldots\ldots \varphi_{p-1},\ \varphi,\ \varphi_1,\ \varphi_2 \ldots\ldots\ldots,$$

oder wenn man durch $\varphi \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^r$ den Werth von φ bezeichnet, welcher entsteht, nachdem die durch $\begin{pmatrix} A_1 \\ A_m \end{pmatrix}$ bezeichnete Verwandlung r mal wiederholt worden, die Reihe

$$\varphi \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^0,\quad \varphi \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^1,\quad \varphi \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^2 \ldots\ldots \varphi \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{p-1},\quad \varphi \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^0 \ldots\ldots$$

Hieraus folgt, dafs

$$\varphi \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{\alpha p + r} = \varphi \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^r$$

$$\varphi \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{\alpha p} = \varphi \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^0 = \varphi.$$

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

Es müssen also zwei von den p Werthen

$$\varphi \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^0,\quad \varphi \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^1,\quad \varphi \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^2 \ldots\ldots \varphi \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{p-1}$$

gleich sein. Es sei z. B.

$$\varphi \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^r = \varphi \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{r'},$$

so folgt daraus

$$\varphi \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{r'+p-r} = \varphi \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{r'+p-r}$$

Dieses giebt, weil $\varphi \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^p = \varphi$, wenn man r statt $r' + p - r$ setzt,

$$\varphi = \varphi \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^r;$$

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

$$v = v \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{r\alpha},$$

wo α eine ganze Zahl bedeutet.

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

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

Also ist

$$v = v \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{p\beta+1},$$

oder weil $v = v \begin{pmatrix} A_1 \\ A_m \end{pmatrix}^{p\beta}$ war,

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

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

Nun ist klar, dafs

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

zwei wiederkehrende Verwandlungen vom Grade p sind, wenn die Zahl der Zeiger $\alpha, \beta, \gamma \ldots\ldots \eta$ 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

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

folgt.

Man sieht hieraus, dafs die Function φ 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, dafs ein beliebiger Werth von φ durch eine grade Zahl von Versetzungen nicht verändert wird, und dafs folglich alle Werthe von φ, 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 φ kann also nicht mehr als zwei verschiedene Werthe haben. Dieses giebt folgenden Lehrsatz:

> Die Zahl der verschiedenen Werthe einer Function von n Gröfsen kann entweder gar nicht bis unter die gröfste 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 Gröfsen 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 φ und φ' zwei Functionen sein, welche jede zwei verschiedene Werthe haben, so ist dem Vorigen zufolge klar, dafs wenn man durch φ_1, φ_2 und φ_1', φ_2' jene doppelten Werthe bezeichnet, dafs alsdann die beiden Ausdrücke

$$\varphi_1 + \varphi_2 \text{ und } \varphi_1\varphi_1' + \varphi_2\varphi_2'$$

symmetrische Functionen sind. Es sei

$$\varphi_1 + \varphi_2 = t \text{ und } \varphi_1\varphi_1' + \varphi_2\varphi_2' = t_1,$$

so findet man

$$\varphi_1 = \frac{t\cdot\varphi_2' - t_1}{\varphi_2' - \varphi_1'}.$$

Man setze nunmehr die Zahl der Gröfsen $x_1\ x_2 \ldots\ldots x_m$ 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 $v_1' = \varepsilon$, so ist $v_2' = -\varepsilon$. Der Ausdruck von v_1 ist also

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

$$v_1 = \tfrac{1}{2}t_2 + \frac{t_1}{2\varepsilon}\varepsilon,$$

wo $\frac{1}{2}t_2$ eine symmetrische Function ist. ε hat zwei Werthe, die nur dem Zeichen nach verschieden sind, so dafs also $\frac{t_1}{2\varepsilon^2}$ ebenfalls eine symmetrische Function ist. Setzt man also $\frac{1}{2}t_2 = p$ und $\frac{t_1}{2\varepsilon_2} = q$, so folgt

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

$$\varepsilon = (x_1 - x_2)(x_3 - x_3) \ldots\ldots (x_4 - x_5)$$

ist.

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

Es sei v eine rationale Function der Gröfsen x_1, x_2, x_3, x_4, x_5, welche die Eigenschaft hat, unveränderlich zu sein, wenn man beliebige vier von den fünf Gröfsen 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 Gröfse 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

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

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

Daraus folgt, dafs 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 Gröfse; 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, dafs man

$$v = r_0 + r_1 x_1 + r_2 x_1^2 \ldots\ldots\ldots + r_m x_1^m$$

setzen kann. Multiplicirt man die Gleichung

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

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

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

in welchen α, β, γ, δ, ε rationale Functionen von a, b, c, d, e sind.

Man kann also v auf die Form

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

bringen, wo r_0, r_1, r_2 etc. rationale Functionen von a, b, c, d, e sind, das heifst 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 Gröfsen 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 Gröfsen 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, dafs 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 1.2.3.4.5. Bezeichnet man also durch μ die Zahl der Werthe, welche v bekommt, wenn man die Gröfsen x_2, x_3, x_4, x_5 unter einander vertauscht, so mufs 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

$$\begin{aligned} v_1 + v_2 &= \varphi(x_1) \\ v_2 + v_3 &= \varphi(x_2) \\ &\cdots\cdots\cdots \\ v_{m-1} + v_m &= \varphi(x_{m-1}) \\ v_m + v_1 &= \varphi(x_m), \end{aligned}$$

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

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

welches

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

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

4. Es

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, dafs diese Voraussetzung nicht Statt findet. Also kann auch nicht $\mu = 3$ sein.

Zusammengenommen also findet man folgenden Lehrsatz:

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

$$r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4,$$

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

Aus

$$r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4 = v$$

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

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

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 ..... v_m hat. Setzt man

$$(v - v_1)(v - v_2)(v - v_3) ..... (v - v_m)$$
$$= q_0 + q_1 v + q_2 v^2 ..... + q_{m-1} v^{m-1} + v^m = 0,$$

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

$$t_0 + t_1 v + t_2 v^2 ..... + t_{\mu-1} v^{\mu-1} + v^\mu = 0$$

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

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

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

$$v^\mu + t_{\mu-1} v^{\mu-1} ..... = (v - v_2) . P_2,$$
$$v^\mu + t_{\mu-1} v^{\mu-1} ..... = (v - v_3) . P_3,$$
$$.....$$
$$v^\mu + t_{\mu-1} v^{\mu-1} ..... = (v - v_m) . P_m.$$

Daraus folgt, dafs $v - v_1$, $v - v_2$, $v - v_3$ ..... $v - v_m$ sämmtlich Factoren

von $\varphi^\mu + t_{\mu-1}\varphi^{\mu-1} \ldots\ldots$ sind, und dafs folglich μ nothwendig gleich m sein mufs. Man erhält daher folgenden Lehrsatz:

Wenn eine rationale Function mehrerer Gröfsen m verschiedene Werthe hat, so läfst 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 zusammengenommen läfst sich behaupten:

dafs 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 mufs

$$R^{\frac{1}{m}} = \varrho$$

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

$$\varrho^m - R = 0$$

und da es zufolge (§. II.) unmöglich ist, den Grad dieser Gleichung zu erniedrigen, so wird die Function ϱ, 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 mufs, so kann m gleich 2, 3 oder 5 sein. Nun existirt aber zufolge (§. III.) keine Function von fünf Gröfsen, welche 3 Werthe hat: es mufs also $m = 5$ oder $m = 2$ sein. Es sei $m = 5$; so erhält man, zufolge des vorigen Paragraphs,

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

und hieraus

$$x = s_0 + s_1 R^{\frac{1}{5}} + s_2 R^{\frac{2}{5}} + s_3 R^{\frac{3}{5}} + s_4 R^{\frac{4}{5}}.$$

Nach (§. II.) folgt daraus

$$s_1 R^{\frac{1}{5}} = x_1 + \alpha^4 x_2 + \alpha^3 x_3 + \alpha^2 x_4 + \alpha x_5,$$

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

Es muſs also $m = 2$ sein.

Alsdann ist nach (§. II.)

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

wo p und q symmetrische Functionen sind, und

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

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 $\alpha + \beta . \sqrt{s^2} = \alpha + \beta s$ 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

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

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

$$\sqrt[m]{(\alpha + \beta s)} = \varrho_1 \text{ und } \sqrt[m]{(\alpha - \beta s)} = \varrho_2,$$

wo ϱ_1 und ϱ_2 rationale Functionen sind. Multiplicirt man ϱ_2 mit ϱ_1 so erhält man $\varrho_2 \varrho_1 = \sqrt[m]{(\alpha^2 - \beta^2 s^2)}$.

Nun ist $\alpha^2 - \beta^2 s^2$ eine symmetrische Function. Wenn also $\sqrt[m]{(\alpha^2 - \beta^2 s^2)}$ nicht eine symmetrische Function wäre, so müſste, dem Obigen zufolge, $m = 2$ sein. Alsdann aber ist $\varrho = \sqrt{(\alpha + \beta \sqrt{s^2})}$, und ϱ 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

$$\varrho_2 \varrho_1 = \gamma \text{ und } \varrho_2 = \frac{\gamma}{\varrho_1}.$$

Nun nehme man den Ausdruck

$$\varrho_1 + \varrho_2 = \sqrt[m]{(\alpha + \beta \sqrt{s^2})} + \frac{\gamma}{\sqrt[m]{(\alpha + \beta \sqrt{s^2})}} = p$$

$$= \sqrt[m]{R} + \frac{\gamma}{\sqrt[m]{R}} = R^{\frac{1}{m}} + \frac{\gamma}{R} R^{\frac{m-1}{m}}.$$

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

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

ist, durch p_1, p_2 ..... p_m, und mache das Product

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

so ist leicht zu sehen, dafs 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 mufs 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 heifst, 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 $p = t_2 R^{\frac{2}{5}}$ folgt aber $p^5 = t_1^5 R$, und weil $t_2^5 R$ von der Form $u + u' \sqrt{s^2}$ ist, $p^5 = u + u' \sqrt{s^2}$, welches

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

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

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

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

Wir schliefsen aus diesem Allen:

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

Daraus folgt unmittelbar weiter, dafs 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.