ÜBER DIE BEZIEHUNGEN,

WELCHE

ZWISCHEN DEN WURZELN IRREDUCTIBELER GLEICHUNGEN

STATTFINDEN,

INSBESONDERE WENN DER GRAD DERSELBEN EINE PRIMZAHL IST.

VON THEODOR SCHÖNEMANN,
MATHEMATICUS AM GYMNASIUM ZU BRANDENBURG A. H.

(GELESEN IN DER SITZUNG DER MATHEMATISCH-NATURWISSENSCHAFTLICHEN CLASSE AM XIX. APRIL MDCCCLII.)

Ungefähr zwei Jahre, nachdem meine Abhandlung: „Grundzüge einer allgemeinen Theorie der höheren Congruenzen etc." (Crelle's Journal, Bd. 31) erschienen war, machte mich der leider zu früh verstorbene Professor Jacobi darauf aufmerksam, dass der Hauptsatz jener Abhandlung bereits von Galois aufgezeichnet sei in der Abhandlung: *Sur la théorie des nombres*, Seite 14 der von J. Liouville herausgegebenen *„Oeuvres mathématiques d'Evariste Galois." (Extrait du Journal de Mathématiques pures et appliquées, tome XI, 1846)*, und forderte mich zugleich auf, den Principien der algebraischen Untersuchungen von Galois nachzuforschen. Die Dunkelheit dieser Schriften, die mir bis dahin gänzlich unbekannt gewesen waren, bewirkten es, dass ich leider erst nach dem Tode des Prof. Jacobi zu einem Einblick in diese einfachen und tiefen Sätze der höheren Algebra gelangte. Es geschah dies bei dem Beweise eines Satzes, der mir durch gewisse Eigenthümlichkeiten der höheren Congruenzen zu einem hohen Grade der Wahrscheinlichkeit erhoben war. Dieser Satz heisst: Zwischen den Wurzeln einer irreductibelen Gleichung, deren Grad eine Primzahl ist, kann keine Gleichung des ersten Grades mit rationalen Coëfficienten stattfinden, ausser der bekannten, dass die Summe der Wurzeln gleich dem negativen ersten Coëfficienten der irreductibelen Gleichung ist. Indem ich nun in den folgenden Blättern den strengen Beweis dieses Satzes mittheile, habe ich vorzüglich die Absicht, die Principien, von welchen Galois in seinem berühmten, aber bis jetzt noch nicht aufgeklärten *Mémoire sur les conditions de résolubilité des équations par radicaux* (S. 33 der *Oeuvres mathématiques*) ausging, ohne sie vollständig auszuspreehen, in ein klares Licht zu stellen. Ich bemerke sogleich, dass der Satz des §. 1 von Abel herrührt, ebenso der Satz des §. 4, der zugehörige Beweis aber von Galois. Der Satz des §. 6 ist von Galois zwar mehrfach angewendet, aber weder hervorgehoben noch bewiesen worden; eben so verhält es sich mit dem Satze des §. 11.

Auf die übrigen Sätze und Beweise glaube ich einen gerechten Anspruch zu haben, obgleich es höchst wahrscheinlich ist, dass Galois dieselben gekannt und angewendet hat.

§. 1. Erklärung und Lehrsatz. Bedeutet fx irgend eine ganze Function von x, welche sich nicht in der Art in zwei Factoren von niedrigerem Grade zerfällen lässt, dass die Coëfficienten dieser Factoren wieder rationale Functionen der Coëfficienten von fx sind, so heisst fx ein irreductibeler Ausdruck von x.

Wenn fx ein irreductibeler Ausdruck von x ist, so kann derselbe mit keinem anderen Ausdrucke f_1x, dessen Coëfficienten ebenfalls rationale Functionen der Coëffieienten von fx sind, eine Wurzel gemeinschaftlich haben, ohne dass f_1x durch fx ohne Rest theilbar sei.

Beweis. Bestimmt man nach den gewöhnlichen Methoden den grössten gemeinschaftlichen Theiler zwischen fx und f_1x, so ist dieser offenbar ebenfalls ein Ausdruck von x, dessen Coëfficienten rationale Functionen der Coëfficienten von fx sind. Wäre dieser Theiler nun nicht fx selbst, so wäre er von niedrigerem Grade als fx und mindestens vom ersten Grade. Demnach müsste also fx einen solchen Factor haben, was gegen die Voraussetzung ist.

§. 2. Erklärung und Lehrsatz. Sind $\alpha_1, \alpha_2, \ldots \alpha_n$ die Wurzeln des irreductibelen Ausdruckes fx, und bedeutet φx eine rationale Function von x, und den Coëfficienten von fx, so soll der Ausdruck

$$(x-\varphi\alpha_1)\ (x-\varphi\alpha_2)\ldots(x-\varphi\alpha_n)$$

der transformirte Ausdruck von fx heissen, und durch $f_\varphi x$ bezeichnet werden.

Der transformirte Ausdruck ist entweder selbst irreductibel, oder die Potenz eines irreductibelen Ausdruckes.

Beweis. Gesetzt $f_\varphi x$ sei $(ax)^m\, qx$, wo ax und qx rationale Ausdrücke von x und den Coëfficienten von fx bedeuten, und m eine ganze Zahl ist, ferner ax irreductibel und kein Factor von qx ist, so ist auch:

$$f_\varphi(\varphi x) = (\varphi x-\varphi\alpha_1)\ (\varphi x-\varphi\alpha_2)\ldots(\varphi x-\varphi\alpha_n) = [a(\varphi x)]^m\, q(\varphi x)$$

und es muss daher entweder $a(\varphi\alpha_1) = 0$ oder $q(\varphi\alpha_1) = 0$ sein, mithin entweder $a(\varphi x) = fx \cdot q_1x$ oder $q(\varphi x) = fx \cdot q_2x$ sein, wo q_2x und q_1x ebenfalls ganze rationale Functionen von x sind. Im ersten Falle würde

$$a(\varphi\alpha_1) = a(\varphi\alpha_2) = \ldots a(\varphi\alpha_n) = 0,$$

im anderen Falle

$$q(\varphi\alpha_1) = q(\varphi\alpha_2) = \ldots q(\varphi\alpha_n) = 0 \text{ sein.}$$

Setzt man nun statt φx, z, so erhält man

$$(z-\varphi\alpha_1)\ (z-\varphi\alpha_2)\ldots(z-\varphi\alpha_n) = (az)^m\, qz$$

und es müssten für den ersten Fall die Wurzeln von

$$qz = \frac{(z-\varphi\alpha_1)\ (z-\varphi\alpha_2)\ldots(z-\varphi\alpha_n)}{(az)^m},$$

und für den zweiten Fall die Wurzeln von

$$(az)^m = \frac{(z-\varphi\alpha_1)\ (z-\varphi\alpha_2)\ldots(z-\varphi\alpha_n)}{qz}$$

mit gewissen Werthen von $\varphi\alpha_1, \varphi\alpha_2, \ldots \varphi\alpha_n$ zusammen fallen; daher müsste für den ersten Fall $q(\varphi\alpha) = 0$, und für den zweiten $a(\varphi\alpha_\nu) = 0$ werden, wo ν einen der Indices $1, 2, \ldots n$

bedeutet. Daher müsste aber auch für den ersten Fall $q\,(\varphi x)$ und für den zweiten Fall $a\,(\varphi x)$ durch fx ohne Rest theilbar sein (§. 1). Mithin müssten in beiden Fällen $q\,(\varphi x)$ und $a\,(\varphi x)$ durch fx ohne Rest theilbar sein. Setzt man nun $a\,(\varphi x) = fx.q_1x$ und $q\,(\varphi x) = fx.q_2x$, so muss sowohl $a\,(\varphi\alpha_1)$ als auch $q\,(\varphi\alpha_1) = 0$ sein. Mithin haben die Ausdrücke ax und qx die Wurzel $\varphi\alpha_1$ gemeinschaftlich, und es müsste sich daher qx ohne Rest durch ax theilen lassen. Da dies gegen die Voraussetzung ist, so kann gar kein qx existiren, und fx ist $= (ax)^m$.

§. 3. Lehrsatz. Ist fx irgend ein Ausdruck vom Grade n, dessen Coëfficienten rationale Zahlen sind (irreductibel oder nicht), und der nicht zwei gleiche Wurzeln hat, so kann man stets eine unendliche Menge von Primzahlen so bestimmen, dass, wenn man eine von ihnen mit p, und die Wurzeln von fx mit $\alpha_1, \alpha_2, \ldots \alpha_n$ bezeichnet, der Ausdruck

$$\alpha_1 + p\alpha_2 + p^2\alpha_3 + \ldots + p^{n-1}\alpha^n$$

einen andern Werth annehme, wenn man die Ordnung der Werthe $\alpha_1, \alpha_2 \ldots \alpha_n$ ändert, so dass also jener Ausdruck durch sämmtliche mögliche Permutationen 1, 2, 3, $\ldots n$ oder $n!$ verschiedene Werthe annehmen muss.

Beweis. Wir werden zunächst annehmen, dass wenn

$$fx = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n$$

gesetzt wird, $a_0 = 1$ und die übrigen Coëfficienten $a_1, a_2, \ldots a_n$ ganze Zahlen sind. Bildet man nun einen Ausdruck $\Pi\,(x)$ dessen Wurzeln die Differenzen je zweier Wurzeln von fx sind, so ist

$$\begin{aligned}\Pi\,(x) = &\big(x-(\alpha_1-\alpha_2)\big)\big(x-(\alpha_1-\alpha_3)\big)\ldots\big(x-(\alpha_1-\alpha_n)\big)\cdot\\ &\big(x-(\alpha_2-\alpha_1)\big)\big(x-(\alpha_2-\alpha_4)\big)\ldots\big(x-(\alpha_2-\alpha_n)\big)\cdot\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ &\big(x-(\alpha_{n-1}-\alpha_1)\big)\big(x-(\alpha_n-\alpha_2)\big)\ldots\big(x-(\alpha_n-\alpha_{n-1})\big),\end{aligned}$$

und die Coëfficienten von $\Pi(x)$ müssen symmetrische Functionen der Wurzeln $\alpha_1, \alpha_2 \ldots \alpha_n$, mithin wieder ganze Zahlen sein. Setzt man nun voraus, p sei eine Primzahl, die nicht in den letzten Coëfficienten von $\Pi\,(x)$ oder in

$$(\alpha_1-\alpha_2)^2\,(\alpha_1-\alpha_3)^2\ldots(\alpha_1-\alpha_n)^2\,(\alpha_2-\alpha_3)^2\,(\alpha_2-\alpha_4)^2\ldots(\alpha_{n-1}-\alpha_n)^2$$

aufgeht, so genügt sie der eben aufgestellten Bedingung.

Gesetzt nämlich irgend zwei Ausdrücke der obigen Art,

$$\alpha_1 + p\alpha_2 + p^2\alpha_3 + \ldots + p^{n-1}\alpha_n \quad \text{und} \quad p^{\mu_0}\alpha_1 + p^{\mu_1}\alpha_2 + p^{\mu_2}\alpha_3 + p^{\mu_{n-1}}\alpha_n,$$

wo $\mu_0, \mu_1 \ldots \mu_{n-1}$ die Zahlen 0, 1, 2, $\ldots n-1$ in irgend einer Folge nur nicht in der eben hingeschriebenen bedeuten, wären gleich, so wäre die Differenz derselben 0, und man erhielte:

$$\alpha_1\,(1-p^{\mu_0}) + \alpha_2\,(p-p^{\mu_1}) + \ldots \alpha_n(p^{n-1}-p^{\mu_{n-1}}) = 0.$$

Setzt man nun zunächst voraus, μ_0 wäre nicht 0 sondern μ_m, so wäre:

$$\alpha_1 - \alpha_{m+1} = \alpha_1p^{\mu_0} - \alpha_2\,(p-p^{\mu_1}) - \alpha_3\,(p^2-p^{\mu_2})\ldots-\alpha_n\,(p^{n-1}-p^{\mu_{n-1}}) - \alpha_{m+1}.p^m,$$

wo aber in der Reihe der Ausdrücke

$$-\alpha_2\,(p-p^{\mu_1}) - \alpha_3\,(p^2-p^{\mu_2})\ldots-\alpha_n\,(p^{n-1}-p^{\mu_{n-1}}) \text{ der Ausdruck } -\alpha_{m+1}\,(p^m - p^{\mu_m})$$

fehlt. Setzen wir die rechte Seite jener Gleichung $pk\,(\alpha_1\,\alpha_2\,\ldots\,\alpha_n)$, wo $k\,(\alpha_1\,\alpha_2\,\ldots\,\alpha_n)$ eine ganze ganzzahlige Function von den Werthen $\alpha_1\,\alpha_2\,\ldots\,\alpha_n$ bedeutet, so erhalten wir die Gleichung

$$\alpha_1 - \alpha_{m+1} = pk\,(\alpha_1\,\alpha_2\,\ldots\,\alpha_n).$$

Entwickelt man nun die Gleichung für $pk\,(\alpha_1\,\alpha_2\,\ldots\,\alpha_n)$, indem man $\alpha_1,\ \alpha_2\,\ldots\,\alpha_n$ allen möglichen Permutationen unterzieht, und jeden sich ergebenden Werth als eine Wurzel derselben ansieht, so wird diese von der Form:

$$\left[x - p\,k\,(\alpha_1\,\alpha_2\,\ldots\,\alpha_{n-1}\,\alpha_n)\right]\left[x - p\,k\,(\alpha_1\,\alpha_2\,\ldots\,\alpha_n\,\alpha_{n-1})\right]\ldots\left[x - p\,k\,(\alpha_n\,\alpha_{n-1}\,\ldots\,\alpha_2\,\alpha_1)\right]$$
$$= x^P + pZ_1x^{P-1} + p^2Z_2x^{P-2} + \ldots p^PZ_P = 0$$

sein, wo P eine ganze Zahl ist, und $Z_1,\ Z_2,\ \ldots\ Z_P$ als symmetrische Functionen von $\alpha_1\,\alpha_2\,\ldots\,\alpha_n$ ebenfalls ganze Zahlen sein müssen. Diese Gleichung müsste mit $\Pi(x) = 0$ die Wurzel $\alpha_1 - \alpha_{m+1}$ gemeinschaftlich haben. Es müsste mithin das Product:

$$\left[(\alpha_1 - \alpha_2)^P + p\,Z_1\,(\alpha_1 - \alpha_2)^{P-1} + \ldots + p^P\,Z_P\right] \times$$
$$\left[(\alpha_1 - \alpha_3)^P + p\,Z_1\,(\alpha_1 - \alpha_3)^{P-1} + \ldots + p^P\,Z_P\right] \times$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\left[(\alpha_n - \alpha_{n-1})^P + p\,Z_1\,(\alpha_n - \alpha_{n-1}) \quad + \ldots + p^P\,Z_P\right] = 0 \text{ sein.}$$

Hiernach müsste aber:

$$(\alpha_1 - \alpha_2)^P\,(\alpha_1 - \alpha_3)^P \ldots (\alpha_1 - \alpha_n)^P \times$$
$$(\alpha_2 - \alpha_1)^P\,(\alpha_2 - \alpha_3)^P \ldots (\alpha_2 - \alpha_n)^P \times$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$(\alpha_{n-1} - \alpha_1)^P\,(\alpha_n - \alpha_2)^P \ldots (\alpha_n - \alpha_{n-1})^P$$

durch p aufgehen, was nicht möglich ist, da nach der Voraussetzung die p^{te} Wurzel dieses Ausdruckes nicht durch p aufgeht, obschon sie eine ganze Zahl ist.

Ist nun aber $\mu_0 = 0$, $\mu_1 = 1$, $\mu_2 = 2$ etc. und endlich μ_m die erste Zahl die nicht mit m übereinstimmt, und wäre nun

$$\alpha_1 + p\,\alpha_2 + p^2\alpha_3 + \ldots p^{n-1}\alpha_n = p^{\mu_0}\,\alpha_1 + p^{\mu_1}\,\alpha_2 + p^{\mu_2}\alpha_3 + \ldots p^{\mu_{n-1}}\,\alpha_n,$$

so erhält man durch Subtraction und Division mit p^m die Gleichung:

$$\alpha_{m+1} - \alpha_{m_1+1} = (p^{\mu_m - m}\alpha_{m+1} + p^{\mu_{m+1} - m}\alpha_{m+2} + \ldots p^{\mu_{n-1} - m}\alpha_n) - (p\,\alpha_{m+2} + p^2\alpha_{m+3} + \ldots + p^{n-1-m}\alpha_n)$$

wo aber aus der Reihe der Ausdrücke

$$p^{\mu_m - m}\alpha_{m+1} + p^{\mu_{m+1} - m}\alpha_{m+2} + \ldots p^{\mu_{n-1} - m}\alpha \text{ der Ausdruck } p^{\mu_{m_1} - m}\alpha_{\mu_1+1}$$

hinwegzulassen ist. Aber alle Exponenten $\mu_m - m$, $\mu_{m+1} - m$, $\mu_{n-1} - m$ müssen, wenn man eben $\mu_{m_1} - m$ aus ihnen fortlässt, grösser wie 1 sein, und daher lässt sich wie vorher

$$\alpha_{m+1} - \alpha_{m_1+1} = p\,k\,(\alpha_{m+1}\,\alpha_{m+2}\,\ldots\,\alpha_n)$$

setzen, und der Beweis wie oben zu Ende führen.

Sollten unter den Coëfficienten von fx Brüche vorkommen, so setze man

$$fx = x^n + \frac{a_1}{a_0}x^{n-1} + \frac{a_2}{a_0}x^{n-2} + \ldots + \frac{a_n}{a_0}$$

und bestimme a_0, a_1, ... a_n als ganze Zahlen, so erhält man

$$a_0^n f\left(\frac{y}{a_0}\right) = y^n + a_1 y^{n-1} + a_2 a_0 y^{n-2} + a_3 a_0^2 y^{n-3} + \ldots + a_n a_0^{n-1}.$$

Sind nun die Wurzeln von fx nämlich α_1, α_2, ... α_n sämmtlich unter sich verschieden, so sind auch die Wurzeln von

$$y^n + a_1 y^{n-1} + \ldots + a_n a_0^{n-1}$$

unter sich verschieden, weil diese $a_0\alpha_1$, $a_0\alpha_2$, ... $a_0\alpha_n$ sind. Bestimmt man nun aber p so, dass sämmtliche Werthe, die sich aus dem Ausdruck

$$a_0\alpha_1 + p a_0\alpha_2 + \ldots p^{n-1} a_0 \alpha_{n-1}$$

durch Permutation der Grössen $a_0\alpha_1$. $a_0\alpha_2$, ... $a_0\alpha_{n-1}$ ergeben, verschieden werden, so muss dasselbe auch von den Ausdrücken gelten, die aus

$$\alpha_1 + p\alpha_2 + p^2\alpha_3 + \ldots + p^{n-1}\alpha_n$$

durch Permutation von α_1, α_2, ... α_n hervorgehen.

§. 4. Lehrsatz. Haben α_1, α_2, α_3 ... α_n und p die ihnen im vorigen §. ertheilte Bedeutung, so kann man durch jeden Werth von der Form

$$\alpha_{\mu_1} + p\alpha_{\mu_2} + p^2\alpha_{\mu_3} + \ldots + p^{n-1}\alpha_{\mu_n}$$

wo μ_1, μ_2, ... μ_n die Zahlen 1, 2, ... n in irgend welcher Ordnung bedeuten, jeden der Werthe α_1, α_2, ... α_n rational ausdrücken, und mithin jede rationale Function von α_1, α_2, ... α_n als rationale Function jenes Werthes.

Beweis. Bezeichnet man

$$\alpha_{\mu_1} + p\alpha_{\mu_2} + p^2\alpha_{\mu_3} + \ldots + p^{n-1}\alpha_{\mu_n} \text{ durch } V_{(\mu_1\mu_2\mu_3\ldots\mu_n)}$$

und sämmtliche Werthe die $V_{(1\mu_2\mu_3\ldots\mu_n)}$ annehmen kann mit v_1, v_2, v_3 ... $v_{1.2.3..(n-1)}$, indem hier den Zahlen μ_2. μ_3 ... μ_n die Werthe 2, 3, ... n in allen möglichen Ordnungen beigelegt werden, so ist

$$(x - v_1)(x - v_2) \ldots (x - v_{1.2.\ldots(n-1)})$$

ein Ausdruck, der sich nach den Potenzen von $x - \alpha_1$ entwickeln lässt, und dessen Coëfficienten symmetrische Functionen von α_2, α_3, ... α_n sein müssen. Die symmetrischen Functionen von α_2, α_3, ... α lassen sich aber als rationale Functionen von α_1 entwickeln, und man kann mithin

$$(x - v_1)(x - v_2) \ldots (x - v_{1.2.\ldots(n-1)}) = g(x\,\alpha_1)$$

setzen, und hiermit eine Function von x bezeichnen, deren Coëfficienten ganze Functionen von α sind. Bezeichnet man nun sämmtliche Werthe von $V_{(2\mu_1\mu_2\ldots\mu_n)}$, wo μ_1, μ_2, μ_3 ... μ_n die Werthe 1, 3, 4, 5 ... n in irgend welcher Ordnung bedeuten, durch u_1, u_2, u_3, ... $u_{(1.2....n-1)}$, so muss

$$(x - u_1)(x - u_2) \ldots (x - u_{(1.2.3....n-1)}) = g(x_1\,\alpha_2)$$

sein. Setzt man in $g(x_1\,\alpha_1)$ statt x einen der Werthe v_1, v_2, ... $v_{1.2...(n-1)}$, den wir mit v bezeichnen wollen, so verschwindet es, und setzt man statt α_1 das Zeichen für eine Unbekannte etwa y, so kann man sagen dass $g(v, y)$ und fy die Wurzel α_1 gemeinschaftlich haben. Aber $g(v, y)$ und y können keine zweite Wurzel etwa α_2 gemeinschaftlich haben, denn die Wurzeln von $g(x, \alpha_2)$ sind $u_1, u_2, \ldots u_{1.2.3.\ldots n-1}$ und diese sind nach dem vorigen §. von $v_1, v_2, \ldots v_{1.2.3\ldots n-1}$ verschieden.

Da also $g(vy)$ und fy nur die Wurzel α_1 gemeinschaftlich haben können, so lässt sich diese durch die Methode den grössten gemeinschaftlichen Factor zwischen $g(v, y)$ und fy zu finden, rational entwickeln.

Es ist wohl zu bemerken, dass das Resultat der Entwickelung dasselbe sein muss, welcher besondere Werth auch v von den Werthen $v_1, v_2, \ldots v_{1.2..(n-1)}$ sein mag. Setzt man also $\alpha_1 = \gamma v$, wo γ eine rationale Function von v bedeutet, so erhält man

$$\alpha_1 = \gamma v_1 = \gamma v_2 = \gamma v_3 = \ldots = \gamma v_{1.2.\ldots(n-1)}.$$

Zugleich folgt aber auch dass

$$\alpha_2 = \gamma u_1 = \gamma u_2 = \gamma u_3 = \ldots = \gamma u_{1.2.\ldots(n-1)}$$

sein müsse, weil die eben angedeuteten Operationen in u, wie in v gemacht werden, wenn man α_2 an die Stelle von α_1 setzt. Eine gleiche Bemerkung gilt natürlich für die anderen Gruppen von Werthen die V annehmen kann.

Anmerkung. Da in γv nach der Natur seiner Entwickelung ein Zähler und ein Nenner enthalten sein muss, die beide rationale ganze Functionen von v sind, so kann man $\gamma v = \frac{\delta v}{\varepsilon v}$ setzen und δv und εv als ganze Functionen von v ansehen. Es ist mithin

$$\gamma v_1 = \frac{\delta v_1 (\varepsilon v_2 . \varepsilon v_3 \ldots \varepsilon v_{1.2.\ldots(n-1)})}{\varepsilon v_1 . \varepsilon v_2 . \varepsilon v_3 \ldots \varepsilon v_{1.2.\ldots(n-1)}}.$$

Aber $\varepsilon v_1 \varepsilon v_2 \varepsilon v_3 \ldots \varepsilon v_{1.2.\ldots(n-1)}$ ist in Bezug auf $\alpha_2, \alpha_3, \ldots \alpha_n$ symmetrisch, man kann es also gleich einer ganzen Function von α_1 oder gleich $\varphi\alpha_1$ setzen. Man erhält mithin:

$$\gamma v_1 = \frac{\delta v_1 (\varepsilon v_2 \varepsilon v_3 \varepsilon v_4 \ldots \varepsilon v_{1.2.\ldots(n-1)}) (\varepsilon u_1 . \varepsilon u_2 \ldots \varepsilon u_{1.2.\ldots(n-1)})}{\varphi\alpha_1 \; \varphi\alpha_2 \ldots \varphi\alpha_n} \text{ etc.}$$

Der Nenner dieses Ausdruckes ist aber offenbar eine rationale Function der Coëfficienten von fx, die man durch Z bezeichnen kann, und

$$(\varepsilon v_2 . \varepsilon v_3 \ldots \varepsilon v_{1.2.\ldots(n-1)}) \; (\varepsilon u_1 . \varepsilon u_2 \ldots \varepsilon u_{1.2.\ldots(n-1)}) \quad \text{etc.}$$

muss sich als rationale Function von v_1 darstellen lassen, da die Coëfficienten der Gleichung für v_1 rationale Functionen der Coëfficienten von fx sind. Bezeichnet man nun das Product von dieser Function mit δv_1 durch ρv_1 so ist $\gamma v_1 = \frac{\rho v_1}{z}$. Es lässt sich mithin die Function γv_1 stets als ganze Function von v_1 ansehen, deren Coëfficienten aber gebrochene Functionen der Coëfficienten von fx sind.

§. 5. Lehrsatz. Setzt man:

$$\begin{aligned}
&1)\ \alpha_1 + p\alpha_2 + p^2\alpha_3 + \ldots + p^{n-1}\alpha_n = V_1\\
&2)\ \alpha_2 + p\alpha_3 + p^2\alpha_4 + \ldots + p^{n-1}\alpha_1 = V_2\\
&3)\ \alpha_3 + p\alpha_4 + p^2\alpha_5 + \ldots + p^{n-1}\alpha_2 = V_3\\
&\qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&n)\ \alpha_n + p\alpha_1 + p^2\alpha_2 + \ldots + p^{n-1}\alpha_{n-1} = V_n
\end{aligned}$$

so kann man die ganze rationale Function GV_1 von V_1 so bestimmen, dass

$$V_2 = GV_1, \; V_3 = GV_2, \ldots V_n = GV_{n-1} \text{ und } V_1 = GV_1$$

wird, und dass überhaupt wenn

$$\alpha_{\mu_1} + p\alpha_{\mu_2} + p^2\alpha_{\mu_3} + \ldots p^{n-1}\alpha_{\mu_n} = U_1$$

gesetzt wird, wo $\mu_1, \mu_2, \ldots \mu_n$ die Zahlen $1, 2, \ldots n$ in irgend welcher Ordnung bedeuten,

$$G\,U_1 = \alpha_{\mu_2} + p\,\alpha_{\mu_3} + p^2\alpha_{\mu_4} + \ldots + p^{n-1}\alpha_{\mu_1}$$

werde.

Beweis. Aus §. 4 ergibt sich dass $\alpha_1 = \gamma V_1$, $\alpha_2 = \gamma V_2$ und überhaupt $\alpha_m = \gamma V_m$ sei. Multiplicirt man nun die zweite Gleichung mit p und zieht sie von der ersten ab, so erhält man:

$$\alpha_1 (1 - p^n) = V_1 - V_2 p,$$

mithin

$$V_2 = \frac{V_1 + (p^n - 1)\alpha_1}{p} = \frac{V_1 + (p^n - 1)\gamma V_1}{p}.$$

Es ist nun

$$G\,V_1 = \frac{V_1 + (p^n - 1)\gamma V_1}{p},$$

denn durch dieselben Operationen kann man nachweisen, dass $G\,U_1$ oder

$$\frac{U_1 + (p^n - 1)\gamma U_1}{p} = \alpha_{\mu_2} + p\,\alpha_{\mu_3} + p^2\alpha_{\mu_4} + \ldots + p^{n-1}\alpha_{\mu_1} \text{ sei.}$$

Zusatz. Da $\alpha_1 = \gamma V_1$, $\alpha_2 = \gamma V_2$ etc. ist (§. 4), so kann man $\alpha_1 = \gamma V_1$, $\alpha_2 = \gamma G V_1$, $\alpha_3 = \gamma G G V_1 = \gamma G^2 V_1$ und überhaupt $\alpha_m = \gamma G^{m-1} V_1$ setzen.

§. 6. Lehrsatz. Bezeichnet man die Gleichung vom Grade $1 \cdot 2 \cdot 3 \ldots n$, von welcher die verschiedenen Werthe von V Wurzeln sind, durch $FV = 0$, und ist $F_1 V$ ein irreductibeler Factor von FV, und V_1 und V_2 zwei Wurzeln dieses Factors, ist ferner

$$V_1 = \alpha_1 + p\,\alpha_2 + p^2\,\alpha_3 + \ldots + p^{n-1}\alpha_n \text{ und } V_2 = \delta_1 + p\,\delta_2 + p^2\delta_3 + \ldots + p^{n-1}\delta_n,$$

wo $\delta_1, \delta_2, \ldots \delta_n$ die Werthe $\alpha_1, \alpha_2, \ldots \alpha_n$ in irgend einer andern Ordnung darstellen, und die ganze Function von V_1, nämlich KV_1 ist

$$= \alpha_{\mu_1} + p\,\alpha_{\mu_2} + \ldots + p^{n-1}\alpha_{\mu_n},$$

wo $\mu_1, \mu_2, \ldots \mu_n$ die Zahlen $1, 2, 3, \ldots n$ in irgend einer Ordnung darstellen, so ist auch

$$KV_2 = \delta_{\mu_1} + p\,\delta_{\mu_2} + \ldots + p^{n-1}\delta_{\mu_n}.$$

Beweis: Es ist

$$\alpha_{\mu_1} + p\,\alpha_{\mu_2} + \ldots + p^{n-1}\alpha_{\mu_n} = \gamma G^{\mu_1 - 1} V_1 + p\,\gamma G^{\mu_2 - 1} V_1 + \ldots + p^{n-1}\,\gamma G^{\mu_n - 1} V_1,$$

denn

$$\alpha_{\mu_1} = \gamma G^{\mu_1 - 1} V_1, \quad \alpha_{\mu_2} = \gamma G^{\mu_2 - 1} V_1 \text{ etc. (§. 5.)}$$

Dividirt man nun

$$KV_1 \text{ und } \gamma G^{\mu_1 - 1} V_1 + p\,\gamma G^{\mu_2 - 1} V_1 + \ldots + p^{n-1}\,\gamma G^{\mu_n - 1} V_1$$

durch $F_1 V_1$, so müssen die sich ergebenden algebraischen Reste identisch sein, weil man sonst eine Gleichung unter dem Grade von der Gleichung $F_1 V = 0$ erhielte, die mit $F_1 V = 0$ eine Wurzel gemeinschaftlich hätte. (§. 1.) Man kann mithin

$$KV_1 = F_1 V_1 \cdot Q V_1 + R V_1 \text{ und } \gamma G^{\mu_1 - 1} V_1 + p\,\gamma G^{\mu_2 - 1} V_1 + \ldots + p^{n-1}\,\gamma G^{\mu_n - 1} V_1 = F_1 V_1 \cdot Q_1 V_1 + R V_1$$

setzen, wo $Q V_1$, $Q_1 V_1$ und $R V_1$ ganze rationale Functionen von V_1 bedeuten. Ist nun kV_1 eine andere Wurzel desselben irreductibelen Factors $F_1 V$, so ist offenbar auch

$$F_1 k V_1 \cdot Q k V_1 + R k V_1 = F_1 k V_1 \cdot Q_1 k V_1 + R k V_1,$$

weil die ersten Glieder beider Seiten der Gleichung verschwinden und die zweiten identisch sind. Setzt man nun $kV_1 = \delta_1 + p\delta_2 + p^2\delta_3 + \ldots + p^{n-1}\delta_{n-1}$, so erhält man

$$KkV_1 = \gamma G^{\mu_1-1} kV_1 + p\gamma G^{\mu_2-1} kV_1 + \ldots + p^{n-1}\gamma G^{\mu_n-1} kV_1.$$

Es ist aber $\gamma G^{\mu_m-1} kV_1 = \delta_{\mu_m}$ (§. 5) und mithin

$$KkV_1 = \delta_{\mu_1} + p\delta_{\mu_2} + p^2\delta_{\mu_3} + \ldots + p^{n-1}\delta_{\mu_n}.$$

Setzt man für kV_1 den Werth V_2, so ist der Satz bewiesen.

Zusatz. Da sich sämmtliche Werthe, welche durch Permutation der Werthe α, aus V_1 oder $\alpha_1 + p\alpha_2 + \ldots + p^{n-1}\alpha_n$ hervorgehen, als Functionen von $\alpha_1, \alpha_2, \ldots \alpha_n$ ansehen lassen, und diese sämmtlich Functionen von V_1 sind, so lässt sich jede Function von $\alpha_1, \alpha_2, \ldots \alpha_n$ als Function des einen Werthes V_1 ansehen. Sind nun V_1 und V_2 Wurzeln des irreductibelen Factors F_1V_1, und ist $V_2 = kV_1$, so ist auch kV_2 eine Wurzel desselben Factors, denn da $F_1kV_1 = 0$ ist, so muss F_1kV durch F_1V aufgehen, da es mit ihm eine Wurzel gemeinschaftlich hat; man kann mithin $F_1kV = F_1V \,.\, QV$ setzen, wo QV eine ganze rationale Function von V bedeutet, und setzt man in diese Gleichung für V den Werth V_2, so ist $F_1kV_2 = F_1V_2 \,.\, QV_2 = 0$, wesshalb kV_2 ebenfalls eine Wurzel von F_1V sein muss. Bezeichnet man nun kkV_1 durch k^2V_1, kk^2V_1 durch k^3V_1 etc., so müssen sämmtliche Werthe V_1, kV_1, k^2V_1, k^3V_1 etc. Wurzeln von F_1V sein, und da die Anzahl dieser Wurzeln eine beschränkte ist, so müssen sie sich wiederholen. Es ist nun zu untersuchen, nach welchen allgemeinen Gesetzen dies geschehe.

§. 7. Ist V_1 und V_2 bekannt, und setzt man $V_2 = kV_1$, so kann man bereits durch Anwendung des §. 6. k^2V_1, k^3V_1 etc. entwickeln. Einige Beispiele werden hinreichen dieses zu zeigen.

Bezeichnet man $\alpha_1 + p\alpha_2 + \ldots + p^{n-1}\alpha_n$ durch $(1, 2, \ldots n)$ und $\alpha_{\mu_1} + p\alpha_{\mu_2} + p^2\alpha_{\mu_3} + \ldots + p^{n-1}\alpha_{\mu_n}$ durch $(\mu_1, \mu_2, \ldots \mu_n)$, setzt man ferner $n = 5$ und $V_1 = (1, 2, 3, 4, 5)$ und $kV_1 = (2, 4, 5, 1, 3)$, so erhält man folgende Entwickelung:

I. $V_1 = (1, 2, 3, 4, 5)$
$kV_1 = (2, 4, 5, 1, 3)$
$k^2V_1 = (4, 1, 3, 2, 5)$
$k^3V_1 = (1, 2, 5, 4, 3)$
$k^4V_1 = (2, 4, 3, 1, 5)$
$k^5V_1 = (4, 1, 5, 2, 3)$
$k^6V_1 = (1, 2, 3, 4, 5)$,

denn da beim Übergange von V_1 in kV_1 die erste Stelle in die zweite, die zweite in die vierte, die dritte in die fünfte, die vierte in die erste und die fünfte in die dritte überging, so muss auch beim Übergange von kV_1 in k^2V_1 dasselbe geschehen, also 2 welches die erste Stelle inne hatte in 4 übergehen, welches in kV_1 die zweite Stelle inne hat, 4 welches die zweite Stelle inne hatte in 1 übergehen, welches in kV_1 die vierte Stelle inne hat etc. (§. 6). Auf gleiche Weise sind folgende Beispiele gebildet:

II. $V_1 = (1, 2, 3, 4, 5)$
$kV_1 = (2, 1, 4, 5, 3)$
$k^2V_1 = (1, 2, 5, 3, 4)$
$k^3V_1 = (2, 1, 3, 4, 5)$
$k^4V_1 = (1, 2, 4, 5, 3)$
$k^5V_1 = (2, 1, 5, 3, 4)$
$k^6V_1 = (1, 2, 3, 4, 5)$

III. $V_1 = (1, 2, 3, 4, 5)$
$kV_1 = (2, 3, 5, 1, 4)$
$k^2V_1 = (3, 5, 4, 2, 1)$
$k^3V_1 = (5, 4, 1, 3, 2)$
$k^4V_1 = (4, 1, 2, 5, 3)$
$k^5V_1 = (1, 2, 3, 4, 5)$

IV. $V_1 = (1, 2, 3, 4, 5)$
$kV_1 = (2, 4, 5, 3, 1)$
$k^2V_1 = (4, 3, 1, 5, 2)$
$k^3V_1 = (3, 5, 2, 1, 4)$
$k^4V_1 = (5, 1, 4, 2, 3)$
$k^5V_1 = (1, 2, 3, 4, 5)$

§. 8. Lehrsatz. Wenn beim Übergange von V_1 in kV_1 α_q in α_r übergeht, so geht auch beim Übergange von kV_1 in k^2V_1, α_q in α_r über, wesshalb dasselbe stattfinden muss, wenn k^mV_1 in $k^{m+1}V_1$ übergeht, wo q und r irgend welche von den Indices $1, 2, \ldots n$ bedeuten und m irgend eine ganze Zahl ist.

Beweis. Bezeichnet man V_1 oder $\alpha_1 + p\alpha_2 + p^2\alpha_3 + p^{n-1}\alpha_n$ durch $(\alpha_1\ \alpha_2 \ldots \alpha_m \ldots \alpha_q \ldots \alpha_n)$ und kV_1, in welchem an die Stelle von α_m der Werth α_q und an die Stelle von α_q der Werth α_r getreten ist, durch $(\ldots\ \alpha_q \ldots\ldots \alpha_r \ldots\ldots)$, so kann man in diesem letzteren Ausdrucke alle Werthe von α als Functionen von V_1 ansehen, und erhält

$$kV_1 = (\ldots\ldots \gamma G^{q-1}V_1 \ldots\ldots \gamma G^{r-1}V_1 \ldots\ldots)$$

und mithin

$$k^2V_1 = (\ldots\ldots \gamma G^{q-1}kV_1 \ldots\ldots \gamma G^{r-1}kV_1 \ldots\ldots).$$

Es ist aber $\gamma G^{q-1}kV_1 = \alpha_r$, denn α_r nimmt die q^{te} Stelle in kV_1 ein. Man erhält mithin die drei Gleichungen

$$\begin{aligned} V_1 &= (\alpha_1\ \alpha_2 \ldots \alpha_m \ldots \alpha_q \ldots \alpha_n) \\ kV_1 &= (\ldots\ldots \alpha_q \ldots \alpha_r \ldots\ldots) \\ k^2V_1 &= (\ldots\ldots \alpha_r \ldots\ldots\ldots) \end{aligned}$$

wodurch der Satz bewiesen ist.

§. 9. Da die Anzahl der verschiedenen Werthe von V_1, kV_1, k^2V_1 etc. eine beschränkte ist (§. 6, Zusatz), so muss für irgend welche ganzzahlige Werthe von m und m_1 der Fall eintreten, dass $k^{m+m_1}V_1 = k^mV_1$ wird. Ist nun m_1 die kleinste Zahl, welche dieser Gleichung genügt, so muss auch $k^{m_1}V_1 = V_1$ sein, denn da

$$k^{m+m_1}V_1 - k^mV_1 = k^{m_1}k^mV_1 - k^mV_1 = 0$$

ist, und k^mV_1 wie oben bewiesen eine Wurzel des irreductibelen Factors F_1V ist, so kann man in jene Gleichung jede andere Wurzel von F_1V einsetzen. Setzt man also für k^mV_1 den Werth V_1, so erhält man $k^{m_1}V_1 - V_1 = 0$. Es wird mithin immer eine kleinste Zahl m^1 geben, die der Gleichung genügt $k^{m_1}V_1 = V_1$. Ist diese einmal bestimmt und x und y bedeuten ganze Zahlen, so wird $k^xV_1 = k^yV_1$ sein, wenn $x \equiv y$ (Mod. m_1) ist. Die Folge der Werthe $V_1, kV_1, k^2V_1, \ldots k^{m_1-1}V_1$ soll eine Periode heissen.

Kennt man V_1 und kV_1, so ist es leicht die Bildungsweise der folgenden Werthe, und die Zahl der Glieder oder m_1 kennen zu lernen. Betrachtet man zu dem Ende das letzte Beispiel des §. 7, nämlich:

$$\begin{aligned} V_1 &= (1, 2, 3, 4, 5) \\ kV_1 &= (2, 4, 5, 3, 1) \\ k^2V_1 &= (4, 3, 1, 5, 2) \\ k^3V_1 &= (3, 5, 2, 1, 4) \\ k^4V_1 &= (5, 1, 4, 2, 3) \\ k^5V_1 &= (1, 2, 3, 4, 5), \end{aligned}$$

so geht beim Übergange von V_1 in kV_1 1 in 2, 2 in 4, 4 in 3, 3 in 5, 5 in 1 über. Durch Anwendung des §. 8 ist hierdurch die Folge der Zahlen in der ersten Verticalreihe der Parenthesen auf der rechten Seite bestimmt, und muss sein 1, 2, 4, 3, 5, 1. Ebenso ist in diesem Beispiel die Folge der Zahlen in der zweiten Verticalreihe bestimmt und ist 2, 4, 3, 5, 1, 2 etc. Fügt man zu jeder Ziffer von V_1 die unter ihr stehende von kV_1 auf folgende Weise [1.2, 2.4, 4.3, 3.5, 5.1], so soll dies Zeichen der Index der Periode heissen. Läuft die erste Ziffer durch alle n Ziffern hindurch ehe sie in sich zurückkehrt, so muss offenbar die Periode aus n, hier also aus fünf Gliedern bestehen. Kehrt die erste

Ziffer aber bereits früher in sich zurück, so muss der Index in mehrere Abtheilungen zerfallen. Da also im ersten Beispiel des §. 7 $V_1 = (1, 2, 3, 4, 5)$ und $kV_1 = (2, 4, 5, 1, 3)$ ist, so bildet sich hier der Index $[1 . 2 , 2 . 4 , 4 . 1 \mid 3 . 5 , 5 . 3]$ der aus zwei Abtheilungen besteht. Hieraus folgt, dass bei diesem Beispiele die erste Verticalreihe aus den Ziffern 1, 2, 4, 1, 2, 4, 1, die zweite aus 2, 4, 1, 2, 4, 1, 2, die vierte aus 4, 1, 2, 4, 1, 2, 4, die dritte aus 3, 5, 3, 5, 3, 5, 3 und die fünfte aus 5, 3, 5, 3, 5, 3, 5 bestehen müsse. Die ganze Periode muss aber offenbar 3×2 Glieder in sich schliessen, weil sie aus zwei einfachen Perioden von drei und zwei Gliedern gebildet ist.

Aus diesen Beispielen geht nun offenbar der Satz hervor: dass wenn der Index für n Wurzeln in m Theile zerfällt, von denen der erste m_1, der zweite m_2, der dritte m_3, . . . der letzte m_n Ziffern in sich schliesst, wo also $n = m_1 + m_2 + m_3 + \ldots m_n$ ist, — dass alsdann die Periode so viele Glieder in sich schliessen wird, als das kleinste Vielfache von $m_1, m_2, \ldots m_n$ angibt.

§. 10. Lehrsatz. Haben fx, $\alpha_1, \alpha_2, \ldots \alpha_n$, p und V die ihnen in den vorigen §§. beigelegte Bedeutung, so ist V im Allgemeinen die Wurzel einer Gleichung vom Grade $1 . 2 . 3 \ldots . n$, deren Coëfficienten rationale Functionen der Coëfficienten von fx sind. Ist nun fx irreductibel und jene Gleichung für V ist $FV = 0$, ist ferner $FV = F_1 V . F_2 V \ldots F_m V$, und die Factoren auf der rechten Seite sind sämmtlich rationale und irreductibele ganze Functionen von V, so sind alle diese Factoren von gleich hohem Grade, und dieser Grad selbst ist ein Vielfaches von n.

Beweis. Setzt man $\alpha_1 + p\alpha_2 + \ldots + p^{n-1}\alpha_n = V_1$ und nimmt an, V_1 sei eine Wurzel von $F_1 V = 0$, so ist $\gamma V_1 = \alpha_1$ (§. 4), mithin haben $F_{1\gamma}V$ und fx die Wurzel α_1 gemeinschaftlich, und es muss daher $F_{1\gamma}V$ gleich einer Potenz von fV sein (§. 2). Da aber $F_{1\gamma}V$ von demselben Grade wie FV ist, so muss dieser ein Vielfaches von n sein.

Wollte man nun voraussetzen $F_1 V$ und $F_2 V$ wären von verschiedenem Grade, so mag $F_1 V$ von geringerem Grade als $F_2 V$ sein. Es sei nun eine Wurzel von $F_2 V$, V_2 so kann man V_2 als rationale Function von V_1 ansehen, da sich alle Wurzeln von FV_1 durch jede rational ausdrücken lassen. Setzt man daher $V_2 = kV_1$, so muss $F_{1k}V$ mit $F_2 V$ eine Wurzel gemeinschaftlich haben, desshalb müsste $F_{1k}V$ eine Potenz von $F_2 V$ sein (§. 2), und der Grad von $F_{1k}V$ wäre mithin ein Vielfaches von dem Grade von $F_2 V$. Der Grad von $F_{1k}V$ stimmt aber überein mit dem Grade von $F_1 V$, und es müsste daher die kleinere Zahl ein Vielfaches der grösseren sein.

§. 11. Lehrsatz. Die Substitutionen, vermöge welcher eine Wurzel des Ausdruckes $F_1 V$ in eine andere desselben Ausdruckes übergeht, sind dieselben wie in jedem der andern Ausdrücke $F_2 V, F_3 V \ldots F_m V$.

Beweis. Gesetzt

$$\alpha_1 + p\alpha_2 + p^2\alpha_3 \ldots . p^{n-1}\alpha_n \text{ und } \delta_1 + p\delta_2 + p^2\delta_3 + \ldots . + p^{n-1}\delta_n$$

seien zwei Wurzeln von $F_1 V$, wo $\delta_1, \delta_2, \ldots \delta_n$ mit $\alpha_1, \alpha_2, \ldots \alpha_n$ bis auf die Ordnung übereinstimmt, und eine Wurzel von $F_2 V$ sei die ganze und rationale Function k von $\alpha_1 + p\alpha_2 \ldots p^{n-1}\alpha_n$, so muss $F_2 V = F_k V$ sein (§. 2, 10). Mithin sind zwei Wurzeln von $F_2 V$ die folgenden beiden:

$$k(\alpha_1 + p\alpha_2 + p^2\alpha_3 + \ldots p^{n-1}\alpha_n) \text{ und } k(\delta_1 + p\delta_2 + p^2\delta_3 + \ldots p^{n-1}\delta_n).$$

Setzt man aber

$$k(\alpha_1 + p\alpha_2 + p^2\alpha_3 + \ldots + p^{n-1}\alpha_n) = \alpha_{\mu_1} + p\alpha_{\mu_2} + \ldots + p^n\alpha_{\mu_n},$$

so ist

$$k(\delta_1 + p\delta_2 + p^2\delta_3 + \ldots + p^{n-1}\delta_n) = \delta_{\mu_1} + p\delta_{\mu_2} + p^2\delta_{\mu_3} + \ldots p^n\delta_{\mu_n}.$$

Die allgemeine Substitution, durch welche

$$\alpha_1 + p\alpha_2 + p^2\alpha_3 + \ldots + p^{n-1}\alpha_n \text{ in } \delta_1 + p\delta_2 + p^2\delta_3 + \ldots p^{n-1}\delta_n$$

übergeht, besteht offenbar darin, dass α_i durch δ_i substituirt wird, wo i einen der Indices $1, 2, 3, \ldots n$ bedeutet, und die allgemeine Substitution, durch welche

$$\alpha_{\mu_1} + p\alpha_{\mu_2} + p^2\alpha_{\mu_3} + \ldots + p^{n-1}\alpha_{\mu_n} \text{ in } \delta_{\mu_1} + p\delta_{\mu_2} + p^2\delta_{\mu_3} + \ldots + p^{n-1}\delta_{\mu_n}$$

übergeht, besteht darin, dass α_{μ_i} durch δ_{μ_i} substituirt wird. Offenbar ist aber die Bedeutung dieser Substitutionen dieselbe.

Zusatz. Es folgt hieraus, dass die Indices der Perioden, welche in $F_1 V$ enthalten sind, durch blosse Veränderungen der Abtheilungen, in die Indices der Perioden übergehen, welche in $F_2 V$ enthalten sind, oder dieselben sind, und dass daher die Perioden, welche in den einzelnen Factoren $F_1 V$, $F_2 V$, $\ldots F_m V$ enthalten sind, aus gleich vielen Gliedern bestehen müssen.

§. 12. Lehrsatz. Ist fx irreductibel und vom Grade n, ist n eine Primzahl, und sind $\alpha_1, \alpha_2, \ldots \alpha_n$ die Wurzeln von fx, haben ferner V, FV, $F_1 V$, $F_2 V$, $\ldots F_m V$ und GV die frühere Bedeutung (§. 10. §. 5), so muss einer der Factoren $F_1 V$, $F_2 V$, $\ldots F_m V$ die Periode V_1, GV_1, $G^2 V_1 \ldots G^{n-1} V_1$ in sich schliessen, d. h. alle diese Werthe müssen zu seinen Wurzeln gehören, wenn V_1 eine dieser Wurzeln ist.

Beweis. Die Ausdrücke $F_1 V$, $F_{1_G} V$, $F_{1_{G^2}} V$, $\ldots F_{1_{G^{n-1}}} V$ sind entweder sämmtlich unter einander verschieden, oder sämmtlich gleich; denn wären zwei Ausdrücke dieser Art gleich, so erhielte man eine Gleichung von der Form:

$$F_{1_{G^{x+y}}} V_1 = F_{1_{G^x}} V,$$

wo x und $x + y$ Zahlenwerthe aus der Reihe $0, 1, 2, 3, \ldots n-1$ sind.

Bestimmt man nun z so, dass $x + y + z = n$ ist, so muss $F_1 V = F_{1_{G^{x+z}}} V$ sein. Da nämlich $F_{1_{G^{x+y}}} V = F_{1_{G^x}} V$ ist, so muss man auch dieselben Ausdrücke erhalten, wenn man in beiden Ausdrücken statt ihrer Wurzeln, dieselben rationalen Functionen G^z dieser Wurzeln setzt. Das Resultat dieser Operation ist aber offenbar durch die Gleichung

$$F_{1_{G^{x+y+z}}} V = F_{1_{G^{x+z}}} V$$

ausgedrückt. Da nun aber $x + y + z = n$ ist, und $G^n V = V$ sein muss, wenn V einen Werth von der Form

$$\alpha_1 + p\alpha_2 + p^2\alpha_3 + \ldots + p^{n-1}\alpha_n$$

bedeutet, so muss

$$F_{1_{G^n}} V = FV$$

sein, und man erhält

$$F_{1_{G^{x+z}}} V = F_1 V.$$

Setzt man nun statt $x + z$ den Buchstaben s, so folgen aus der Gleichung $F_1 V = F_{1_{G^s}} V$ die folgenden

$$F_{1_{G^s}} V = F_{1_{G^{2s}}} V \;,\; F_{1_{G^{2s}}} V = F_{1_{G^{3s}}} V \text{ etc.},$$

welche man aus der ersten Gleichung erhält, wenn man statt ihrer Wurzeln die rationalen Functionen G^s, G^{2s}, G^{3s} etc. hinter einander einsetzt. Da aber s oder $x + z$ kleiner als n sein muss, so sind die Werthe s, $2s$, $3s$, $\ldots (n-1)s$ sämmtlich nach dem Model n verschieden, oder lassen durch n getheilt verschiedene Reste. Offenbar wird aber $G^{is} V = G^r V$ sein, wenn $is \equiv r$ (Model n) ist; aus gleichem Grunde muss $F_{1_{G^{is}}} V = F_{1_{G^r}} V$ sein, wenn $is \equiv r$ (Model n) ist. Legt man aber dem i alle Werthe von 1 bis $n - 1$ bei, so wird man dem Reste r dieselben Werthe beizulegen haben, wenn auch in anderer Ordnung. Durch die Gleichungen

$$F_1 V = F_{1_{G^s}} V = F_{1_{G^{2s}}} V \text{ etc.},$$

ist also dasselbe ausgedrückt wie durch die Gleichungen:

$$F_1V = F_{1_G}V = F_{1_G{}^2}V = F_{1_G{}^3}V \text{ etc.},$$

woher diese letzten stattfinden müssen, wenn

$$F_{1_G{}^{x+y}}V_1 = F_{1_G{}^x}V_1 \text{ ist.}$$

Es muss nun aber nothwendig eine von den folgenden Gleichungen stattfinden:

$$F_1V = F_{1_G}V \;,\; F_2V = F_{2_G}V \;.\;.\;.\;.\; F_mV = F_{m_G}V.$$

Gesetzt nämlich, F_1V wäre nicht gleich $F_{1_G}V$, so wären die Ausdrüeke F_1V, $F_{1_G}V$, $F_{1_G{}^2}V$, . . . $F_{1_G{}^{n-1}}V$ n versehiedene Ausdrüeke aus der Zahl der Ausdrücke F_1V, F_2V, . . . F_mV. Bezeichnet nun $F_\mu V$ einen jener Ausdrüeke, der nieht in den letzten enthalten ist, so müssten aus gleichem Grunde $F_\mu V$, $F_{\mu_G}V$, $F_{\mu_G{}^2}V$, . . . $F_{\mu_G{}^{n-1}}V$, n andere Ausdrücke aus diesen sein, und es folgt daher nothwendig durch fortgesetzte Schlüsse derselben Art, dass n ein Theiler von m sein müsse, wenn keine von jenen Gleichungen in Erfüllung geht. Setzt man aber den Grad von F_1V gleich nz (§. 10), so ist der Grad von FV gleich der Zahl $m \,.\, nz$, derselbe ist aber auch gleich $1 \,.\, 2 \,.\, 3 \,.\,.\,. \,n$, man erhält mithin die Gleichung

$$m \,.\, nz = 1 \,.\, 2 \,.\, 3 \,.\,.\,. \,n$$

und mithin

$$m = \frac{1 \,.\, 2 \,3 \,.\,.\,. \,(n-1)}{z}.$$

Da aber n eine Primzahl ist, so kann m kein Theiler von n sein, und es muss daher eine der Gleichungen

$$F_1V = F_{1_G}V, \; F_2V = F_{2_G}V \;,\; .\;.\;.\; F_mV = F_{m_G}V$$

bestehen. Wäre nun $F_1V = F_{1_G}V$, und V_1 eine Wurzel von F_1V, so müsste auch nothwendig GV_1 eine Wurzel von F_1V sein ete.

§. 13. Hauptsatz. Ist $fx = 0$ eine irreductibele Gleichung von einem Grade n, der eine Primzahl ist, hat man ferner zwischen den Wurzeln $\alpha_1, \alpha_2, \ldots \alpha_n$ von fx irgend eine rationale Gleichung, deren Coëffieienten so wie die von fx rational sind, so kann man diese Wurzeln so ordnen, dass, wenn man sie durch $\beta_1, \beta_2, \beta_3, \ldots \beta_n$ bezeichnet, und die Gleichung, welche zwischen ihnen besteht, durch $\xi(\beta_1\beta_2\beta_3 \ldots \beta_n) = 0$, nothwendigerweise auch die folgenden $(n-1)$ Gleichungen stattfinden müssen:

$$\xi(\beta_2\,\beta_3\,\beta_4 \ldots \beta_n\,\beta_1) = 0 \;,\; \xi(\beta_3\,\beta_4\,\beta_5 \ldots \beta_1\,\beta_2) = 0 \;.\;.\;.\;.\; \xi(\beta_n\,\beta_1\,\beta_2 \ldots \beta_{n-2}\,\beta_{n-1}) = 0.$$

Beweis. Gesetzt F_1V sei der Faetor von FV, von dem V_1 und GV_1 Wurzeln sind, so ist

$$V_1 = \beta_1 + p\beta_2 + p^2\beta_3 + \ldots p^{n-1}\beta_n \text{ und } GV_1 = \beta_2 + p\beta_3 + p^2\beta_4 + \ldots + p^{n-1}\beta_1.$$

Nun ist aber

$$\beta_1 = \gamma V_1 \;,\; \beta_2 = \gamma GV_1 \;,\; \ldots \beta_n = \gamma G^{n-1}V_1 \text{ (§. 5)};$$

mithin ist

$$\xi(\beta_1\,\beta_2 \ldots \beta_n) = \xi(\gamma V_1, \gamma GV_1, \gamma G^2V_1 \ldots \gamma G^{n-1}V_1) = 0.$$

Da aber auch GV_1 eine Wurzel der irreduetibelen Gleichung $F_1V = 0$ ist, so muss die letzte Gleichung auch stattfinden, wenn man GV_1 statt V_1 setzt (§. 6). Man erhält mithin:

$$\xi(\gamma GV_1, \gamma G^2V_1, \gamma G^3V_1 \ldots \gamma G^nV_1) = 0.$$

Setzt man statt der Ausdrücke unter dem Functionszeichen ξ ihre Werthe, und bedenkt, dass $\gamma G^n V_1 = \beta_1$ sein müsse, so erhält man $\xi\,(\beta_2\,\beta_3\,\ldots\,\beta_n\,\beta_1) = 0$. Würde man statt GV_1 in die obige Gleichung $G^2 V_1$ eingesetzt haben, so würde man $\xi\,(\beta_3\,\beta_4\,\ldots\,\beta_n\,\beta_1\,\beta_2) = 0$ erhalten haben etc.

§. 14. Lehrsatz. Zwischen den Wurzeln einer irreductibelen Gleichung $fx = 0$ von einem Grade n der eine Primzahl ist, kann keine Gleichung des ersten Grades stattfinden, deren Coëfficienten so wie die von fx rational sind — ausser der bekannten Gleichung, dass die Summe der Wurzeln dem negativen Coëfficienten von x^{n-1} in fx gleich sei.

Beweis. Man denke sich die Wurzeln so geordnet, dass man mit ihnen die Substitutionen des vorigen Paragraphen vornehmen kann. Bezeichnet man dieselben nun mit $\beta_1, \beta_2 \ldots \beta_n$ und mit $A_1, A_2 \ldots A_n$ sind sie und M rationale Zahlen, so sei die vorausgesetzte Gleichung des ersten Grades $A_1\,\beta_1 + A_2\,\beta_2 + A_3\,\beta_3 + \ldots\ldots + A_n\,\beta_n - M = 0$. Durch Anwendung des vorigen Paragraphen erhält man folgende n Gleichungen:

$$\begin{array}{l}
A_1\,\beta_1 + A_2\,\beta_2 + A_3\,\beta_3 + \ldots A_{n-1}\,\beta_{n-1} + A_n\,\beta_n = M\\
A_1\,\beta_2 + A_2\,\beta_3 + A_3\,\beta_4 + \ldots A_{n-1}\,\beta_n \quad + A_n\,\beta_1 = M\\
A_1\,\beta_3 + A_2\,\beta_4 + A_3\,\beta_5 + \ldots A_{n-1}\,\beta_1 \quad + A_n\,\beta_2 = M\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
A_1\,\beta_n + A_2\,\beta_1 + A_3\,\beta_2 + \ldots A_{n-1}\,\beta_{n-2} + A_n\,\beta_{n-1} = M
\end{array}$$

Bezeichnet man durch ω eine Wurzel der Gleichung $x^n - 1 = 0$, und multiplicirt die erste der obigen Gleichungen mit 1, die zweite mit ω, die dritte mit ω^2, ... die letzte mit ω^{n-1} und addirt sämmtliche Gleichungen, so erhält man:

$$(\beta_1 + \beta_2\,\omega + \beta_3\,\omega^2 + \ldots + \beta_n\,\omega^{n-1})\,(A_1 + A_2\,\omega^{n-1} + A_3\,\omega^{n-2} + \ldots + A_{n-1}\,\omega^2 + A_n\,\omega)$$
$$= M\,(1 + \omega + \omega^2 + \ldots + \omega^{n-1}).$$

Ist nun ω nicht 1, und man legt ihm hinter einander die Werthe $\omega, \omega^2, \omega^3, \ldots \omega^{n-1}, \omega^n$ bei, und bedenkt, dass $1 + \omega + \omega^2 + \ldots + \omega^{n-1} = 0$ sei, so erhält man folgende n Gleichungen:

$$\begin{array}{l}
(\beta_1 + \beta_2\,\omega + \beta_3\,\omega^2 + \ldots \beta_n\,\omega^{n-1})\,(A_1 + A_2\,\omega^{n-1} + A_3\,\omega^{n-2} + \ldots A_n\,\omega) = 0\\
(\beta_1 + \beta_2\,\omega^2 + \beta_3\,\omega^4 + \ldots \beta_n\,\omega^{2(n-1)})\,(A_1 + A_2\,\omega^{2(n-1)} + A_3\,\omega^{2(n-2)} + \ldots A_n\,\omega^2) = 0\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
(\beta_1 + \beta_2\,\omega^{n-1} + \beta_3\,\omega^{2(n-1)} + \ldots \beta_n\,\omega^{(n-1)^2})\,(A_1 + A_2\,\omega + A_3\,\omega^2 + \ldots A_n\,\omega^{n-1}) = 0\\
(\beta_1 + \beta_2 + \beta_3 + \ldots \beta_n)\,(A_1 + A_2 + A_3 + \ldots + A_n) = n\,.\,M.
\end{array}$$

Sind nun aber die Coëfficienten $A_1, A_2, \ldots A_n$ nicht sämmtlich unter einander gleich, und ist die ganze Zahl $m < n$, so kann kein Ausdruck von der Form

$$A_1 + A_2\,\omega^{m(n-1)} + A_3\,\omega^{m(n-2)} + \ldots A_n\,\omega^m$$

verschwinden, weil bekanntlich die Gleichung

$$1 + x + x^2 + \ldots + x^{n-1} = 0$$

irreductibel ist, wenn n eine Primzahl ist, mithin sämmtliche Wurzeln mit der Gleichung

$$A_1 + A_2\,x^{n-1} + A_3\,x^{n-2} + \ldots A_n\,x = 0$$

gemeinschaftlich haben müsste, wenn jener Ausdruck verschwände, und dies nur stattfinden kann, wenn $A_1 = A_2 = A_3 = \ldots = A_n$ ist. Da nun keiner der rechten Factoren in jenen Gleichungen ver-

schwindet, so müssen alle linken Factoren bis auf den letzten verschwinden. Man erhält mithin folgende $n-1$ Gleichungen:

$$1+\frac{\beta_2}{\beta_1}\omega+\frac{\beta_3}{\beta_1}\omega^2+\ldots\ldots\ldots\frac{\beta_n}{\beta_1}\omega^{n-1}=0$$
$$1+\frac{\beta_2}{\beta_1}\omega^2+\frac{\beta_3}{\beta_1}\omega^4+\ldots\ldots\ldots\frac{\beta_n}{\beta_1}\omega^{2(n-1)}=0$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$1+\frac{\beta_2}{\beta_1}\omega^{n-1}+\frac{\beta_3}{\beta_1}\omega^{2(n-1)}+\ldots\ldots\ldots\frac{\beta_n}{\beta_1}\omega^{(n-1)^2}=0.$$

Fügt man hinzu noch die Gleichung

$$1+1+1+\ldots\ldots\ldots\ldots 1=n$$

und dividirt die erste durch ω^m, die zweite durch ω^{2m} ... die $(n-1)^{te}$ durch $\omega^{(n-1)m}$ und addirt sämmtliche Gleichungen, so erhält man

$$\frac{n\beta_m}{\beta_1}=n \text{ oder } \beta_m=\beta_1.$$

Diese Gleichung kann aber nicht stattfinden, weil eine irreductibele Gleichung nicht gleiche Wurzeln haben kann.

Zusatz. Es lässt sich nun leicht nachweisen, dass $A_1\beta_1+A_2\beta_2+\ldots+A_n\beta_n$ durch jede Permutation ungleicher Werthe der Ausdrücke $A_1, A_2, \ldots A_n$ einen andern Werth annehme. Bezeichnet man nämlich dieselben Werthe, aber in anderer Folge, mit $B_1, B_2, \ldots B_n$, und setzt:

$$A_1\beta_1+A_2\beta_2+\ldots A_n\beta_n=B_1\beta_1+B_2\beta_2+\ldots+B_n\beta_n,$$

so müsste

$$A_1-B_1=A_2-B_2=A_3-B_3=\ldots A_n-B_n$$

gleich irgend einem Zahlwerthe z sein. Dies ist aber unmöglich, weil dadurch, dass man von allen Zahlen $A_1, A_2, \ldots A_n$ einen bestimmten Zahlwerth z abzieht, nothwendigerweise eine andere Zahlenreihe entstehen muss, als $B_1, B_2 \ldots B_n$, die aus den Werthen von $A_1, A_2, \ldots A_n$ zusammengesetzt sein soll.