Bibl. Mathesis 3183.

SUBSTITUTIONENTHEORIE

UND IHRE

ANWENDUNGEN AUF DIE ALGEBRA

VON

Dr. EUGEN NETTO,

A. O. PROFESSOR AN DER KAISER WILHELMS-UNIVERSITÄT
ZU STRASSBURG I. E.

LEIPZIG,
VERLAG VON B. G. TEUBNER.
1882.

Druck von B. G. Teubner in Dresden.

Vorwort.

Die im vorliegenden Buche durchgeführte Darstellung der Substitutionentheorie weicht in mehreren nicht unwesentlichen Punkten von der bisher üblichen ab. Hierbei waren Gesichtspunkte massgebend, welche hervorgehoben werden müssen.

Es ist unzweifelhaft, dass der Kreis der Anwendungen eines Algorithmus sich ausdehnen wird, wenn es gelingt, die Grundlagen und den Aufbau desselben von allen nicht unbedingt geforderten Voraussetzungen zu befreien, und ihm durch die Allgemeinheit der Objekte, mit denen er arbeitet, auch die Möglichkeit des Eingreifens in die verschiedensten Gebiete zu geben. Dass die Theorie der Gruppenbildung eine solche Darstellung zulässt, spricht für ihre weitgreifende Bedeutung und für ihre Zukunft.

Handelt es sich hingegen um die Anwendung eines Hilfsmittels auf ein bestimmt vorgeschriebenes und fest umschriebenes Gebiet, so wird auch die Konstruktion desselben nur diesen einen Zweck zu berücksichtigen haben. Für die fehlende, aber nicht mangelnde Allgemeinheit tritt Loslösung von allem Überflüssigen und erhöhte Brauchbarkeit ein; es wird sich im kleineren Kreise die höhere Wirksamkeit zeigen.

Die nachfolgende Darstellung der Substitutionentheorie ist lediglich darauf berechnet, ein wichtiges Hilfsmittel für algebraische Untersuchungen in elementarer Weise vorzuführen. Durch die von vornherein benutzte Verwendung ganzer Funktionen gelingt es nicht nur, der Theorie der Substitutionen, diesem Operieren mit Operationen, einen greifbaren Untergrund zu geben, sondern auch die Beweise vielfach zu vereinfachen, die Anschauungen zu präcisieren, die Hauptfragen scharf hervorzuheben und — was nicht das Unwichtigste zu sein scheint — den Stoff zu beschränken.

Die beiden umfassenden, bisher publizierten Behandlungen der Substitutionentheorie stammen von J. A. Serret und von C. Jordan.

Die vierte Abteilung der „algèbre supérieure“ von Serret ist diesem Gegenstande gewidmet. Die Verschiedenheit der Methoden hier und dort liess kaum eine Benutzung dieses hoch verdienstlichen Werkes

für unsere Zwecke zu. — Anders ist es dem umfassenden Werke von Jordan, dem „Traité des substitutions et des équations algébriques“ gegenüber. Es waren nicht nur die neuen, grundlegenden Begriffe, welche aufgenommen werden mussten; auch manche Beweise und Gedankenfolgen konnten, wie hier ausdrücklich hervorgehoben werden mag, trotz der Verschiedenheit des Ganges im allgemeinen, passend verwendet werden. Die nicht im „Traité“ enthaltenen Untersuchungen des Herrn Jordan, welche benutzt wurden, sind an den betreffenden Stellen angeführt.

Wenn aber auch manche Einzelheiten auf jenen „Traité“ und auf diese Untersuchungen zurückgeführt werden müssen, so verdankt doch der Verfasser seinem verehrten Lehrer Herrn L. Kronecker die Anschauungen, welche seinem gesamten Werke zu Grunde liegen. Er hat sich bemüht, die Früchte, die ihm aus den Vorlesungen und dem Studium der Abhandlungen dieses Gelehrten, die ihm aus dem anregenden persönlichen Verkehre mit diesem Manne geworden sind, zu verwerten; und er hofft, dass die Spuren hiervon an manchen Stellen seiner Arbeit hervortreten mögen. Eines bedauert er: dass die neueste, bedeutende Publikation des Herrn L. Kronecker: „Grundzüge einer arithmetischen Theorie der algebraischen Grössen“ zu spät erschien, als dass er von derselben den Nutzen hätte ziehen können, den zu ziehen er sich und seinen Lesern gewünscht hätte.

Der Plan des Buches ist folgender:

In der ersten Abteilung sind die Grundzüge der Substitutionentheorie mit steter Berücksichtigung der Theorie der ganzen Funktionen abgeleitet; die analytische Darstellung tritt fast ganz in den Hintergrund, da sie später nur zum Hinweis auf die Gruppen auflösbarer Gleichungen gebraucht wird.

In der zweiten Abteilung werden nach der Festlegung einiger Grundbegriffe als Beispiele die Gleichungen zweiten, dritten und vierten Grades, die Abel'schen und die Galois'schen Gleichungen besprochen. Hierauf folgt ein in arithmetischer Behandlung durchgeführtes Kapitel, über dessen Notwendigkeit am betreffenden Orte einiges gesagt ist. Endlich werden dann die allgemeinen, aber noch elementaren Fragen über auflösbare Gleichungen einer Untersuchung unterzogen.

Strassburg i. E.

Eugen Netto.

Inhaltsverzeichnis.

Erster Abschnitt.

Theorie der Substitutionen und der ganzen Funktionen.

Erstes Kapitel.

Symmetrische oder einwertige Funktionen. Alternierende und zweiwertige Funktionen.

Zweites Kapitel.

Mehrwertige Funktionen und Substitutionengruppen.

Drittes Kapitel.

Die verschiedenen Werte einer mehrwertigen Funktion und ihre algebraischen Beziehungen zu einander.

Viertes Kapitel.

Transitivität und Primitivität. Einfache und zusammengesetzte Gruppen. Isomorphismus.

Fünftes Kapitel.

Algebraische Beziehungen zwischen Funktionen derselben Gruppe. Gattungen mehrwertiger Funktionen.

Sechstes Kapitel.

Die Anzahl der Werte ganzer Funktionen.

Siebentes Kapitel.

Untersuchung einiger besonderer Arten von Gruppen.

Achtes Kapitel.

Analytische Darstellung der Substitutionen. Die lineare Gruppe.

Zweiter Abschnitt.

Anwendung der Substitutionentheorie auf die algebraischen Gleichungen.

Neuntes Kapitel.

Die Gleichungen zweiten, dritten und vierten Grades. Gruppe einer Gleichung. Resolventen.

Zehntes Kapitel.

Die Kreisteilungsgleichungen.

Elftes Kapitel.

Die Abel'schen Gleichungen.

Zwölftes Kapitel.

Gleichungen, bei denen rationale Beziehungen zwischen drei Wurzeln herrschen.

Dreizehntes Kapitel.

Über die algebraische Auflösung der Gleichungen.

Vierzehntes Kapitel.

Die Gruppe einer algebraischen Gleichung.

Fünfzehntes Kapitel.

Algebraisch auflösbare Gleichungen.

Erster Abschnitt.

Theorie der Substitutionen und der ganzen Funktionen.

Erstes Kapitel.

Symmetrische oder einwertige Funktionen. Alternierende und zweiwertige Funktionen.

§ 1. Wir legen unseren Untersuchungen n Elemente $x_1, x_2, \ldots x_n$ zu Grunde, welche durchgehends, so lange nicht ausdrücklich das Gegenteil angegeben wird, als von einander unabhängig angesehen werden sollen. Es ist leicht, aus diesen Elementen ganze Funktionen zu bilden, welche ihre Form nicht ändern, wenn irgendwelche Stellungsänderungen oder Umsetzungen der x_λ untereinander vorgenommen werden. Solche Funktionen sind beispielsweise

$$x_1^{\alpha} + x_2^{\alpha} + x_3^{\alpha} + \ldots + x_n^{\alpha},$$
$$x_1^{\alpha} x_2^{\beta} + x_1^{\alpha} x_3^{\beta} + x_2^{\alpha} x_3^{\beta} + \ldots + x_{n-1}^{\alpha} x_n^{\beta} + x_1^{\beta} x_2^{\alpha} + \ldots + x_{n-1}^{\beta} x_n^{\alpha},$$
$$(x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2 \ldots (x_{n-1} - x_n)^2,$$

u. s. w.

Derartige Funktionen heissen symmetrische Funktionen. Es ist ersichtlich, dass dieselben wie ihre Form so auch ihren Wert nicht ändern, falls man die x_λ irgendwie untereinander vertauscht. In diesem Sinne sind symmetrische Funktionen auch einwertige Funktionen.

Umgekehrt lässt sich nachweisen, dass eine ganze Funktion $\varphi(x_1, x_2, \ldots, x_n)$ der n von einander unabhängigen Grössen $x_1, x_2, \ldots x_n$, welche bei beliebigen Vertauschungen der x_λ untereinander keine Wertänderungen erleidet, auch ihrer Form nach bei jenen Vertauschungen ungeändert bleibt. Wir werden also zeigen:

Lehrsatz I. Jede einwertige ganze Funktion der n von einander unabhängigen Variablen $x_1, x_2, \ldots x_n$ ist in diesen Elementen symmetrisch.

Es sei $\varphi(x_1, x_2, \ldots x_n)$ die gegebene einwertige Funktion der n von einander unabhängigen Grössen $x_1, x_2, \ldots x_n$. Wir ordnen $\varphi(x_1, \ldots x_n)$

nach den Potenzen einer derselben, z. B. nach den Potenzen von x_1 und erhalten so den Ausdruck

$$1) \qquad \varphi(x_1, x_2, \ldots x_n) = \varphi_0 . x_1^{\alpha} + \varphi_1 . x_1^{\alpha-1} + \varphi_2 . x_1^{\alpha-2} + \ldots,$$

in welchen die Koefficienten φ_0, φ_1, φ_2, ... ganze Funktionen von x_2, x_3, $\ldots x_n$ allein sind. Nimmt man nun irgend eine Umstellung unter den Elementen x_λ vor und ordnet dann wiederum nach x_1, so erhält man, da die Funktion φ hierbei ihren Wert nicht ändern soll,

$$2) \qquad \varphi(x_1, x_2, \ldots x_n) = \varphi_0' . x_1^{\beta} + \varphi_1' . x_1^{\beta-1} + \varphi_2' . x_1^{\beta-2} + \ldots$$

Für jedes Spezialsystem von Werten für x_1, x_2, $\ldots x_n$ sind also die rechten Seiten von 1) und 2) einander gleich. Es sei $\gamma > \alpha, \beta$; dann nehmen wir γ Spezialsysteme für die x_1, x_2, $\ldots x_n$ an, in denen die Werte x_2, x_3, $\ldots x_n$ stets dieselben bleiben, während x_1 andere und andere Werte erhält. Infolgedessen bleiben die Koefficienten φ_0, φ_1, φ_2, ... und φ_0', φ_1', φ_2', ... für alle γ Systeme ungeändert. Die beiden ganzen Funktionen der Grade α, β von x_1 stimmen sonach für $\gamma > \alpha, \beta$ Werte der Grösse x_1 überein; folglich sind sie nach einem elementaren Satze einander identisch gleich, und es ist für jede Wahl von x_2, x_3, $\ldots x_n$

$$\alpha = \beta; \quad \varphi_0 = \varphi_0', \quad \varphi_1 = \varphi_1', \quad \varphi_2 = \varphi_2', \ \ldots$$

Sollte also bei den Vertauschungen eine Formänderung eingetreten sein, so kann sie nur innerhalb der φ_λ vorkommen und muss so beschaffen sein, dass gleichwohl der Wert von φ_λ ungeändert bleibt. Es gelten demnach für diese Funktionen φ_λ von $n-1$ Variablen dieselben Voraussetzungen wie sie für $\varphi(x_1 \ldots x_n)$ galten; folglich kann man in derselben Art weiter gehen, indem man z. B. nach den Potenzen von x_2 anordnet u. s. f. Ist man bis zu den Funktionen einer Variablen gekommen, so ist man zu Ende, weil der Satz dann mit dem benutzten Hilfssatze zusammenfällt.

Sind die x_λ nicht von einander unabhängig, so ist der Beweis unanwendbar, und der Satz wird unrichtig. Für $x_1 = x_2 = x_3$ ist z. B. $\varphi(x_1, x_2, x_3) = 2x_1^2 + x_1 x_2 - x_3^2$ einwertig, ohne symmetrisch zu sein.

§ 2. Da es bei unseren Untersuchungen hauptsächlich auf die Verbindungen ankommt, in denen die x_λ auftreten, und wenig auf die Koefficienten, so können wir die symmetrischen Funktionen, in Summanden zerlegt, so reduziert denken, dass nur ein Term das Produkt $x_1^{\alpha} x_2^{\beta} \ldots x_n^{\delta}$ enthält.

Besitzt eine so zubereitete Funktion einen Summanden $c . x_1^{\alpha} x_2^{\beta} \ldots x_n^{\delta}$, so fordert die Unveränderlichkeit der Form, dass alle überhaupt mög-

lichen Glieder vorkommen, welche durch Umstellungen der x_λ aus jenem ersten entstehen können. Erschöpfen diese die Summanden der vorgelegten symmetrischen Funktion noch nicht, so giebt es ein neues Glied $c' x_1^{\alpha'} x_2^{\beta'} \ldots x_n^{\delta'}$, in welchem nicht alle Exponenten $\alpha, \beta, \ldots \delta$ gleich den entsprechenden $\alpha', \beta', \ldots \delta'$ sein können u. s. f. Es zerfällt demzufolge jede symmetrische Funktion in eine Summe von solchen symmetrischen Funktionen, in denen alle Summanden aus einem unter ihnen durch Vertauschungen der Elemente untereinander abgeleitet werden können. Alle diese Summanden sind von demselben Typus oder einander ähnlich. Derartige symmetrische Funktionen sind folglich aus einem beliebigen ihrer Summanden ableitbar und daher durch einen solchen unzweideutig zu charakterisieren. Es geschehe dies dadurch, dass wir vor den bezeichnenden Ausdruck $c x_1^{\alpha} x_2^{\beta} \ldots x_n^{\delta}$ ein S setzen. So bedeutet also $S(x_1^2)$ bei zwei Elementen x_1, x_2 die Summe $x_1^2 + x_2^2$, bei dreien die Summe $x_1^2 + x_2^2 + x_3^2$.

§ 3. Betrachtet man die Elemente $x_1, x_2, \ldots x_n$ als die Wurzeln einer Gleichung n^{ten} Grades, so hat dieselbe die Form

$$3) \qquad f(x) \equiv (x - x_1)(x - x_2) \ldots (x - x_n) = 0,$$

und das Polynom der linken Seite lautet entwickelt

$$4) \quad x^n - (x_1 + x_2 + \ldots + x_n) x^{n-1} + (x_1 x_2 + x_1 x_3 + \ldots + x_{n-1} x_n) x^{n-2} - \ldots \pm x_1 x_2 \ldots x_n = x^n - c_1 x^{n-1} + c_2 x^{n-2} - \ldots \pm c_n.$$

Die Koefficienten sind also einfache ganze, symmetrische Funktionen der x_λ

$$c_1 = S(x_1), \quad c_2 = S(x_1 x_2), \quad \ldots, \quad c_\lambda = S(x_1 \ldots x_\lambda)$$
$$c_n = S(x_1 x_2 \ldots x_n) = x_1 x_2 \ldots x_n.$$

Diese Bildungen werden als elementare symmetrische Funktionen bezeichnet. Sie sind dadurch von Wichtigkeit, dass jede ganze symmetrische Funktion der x_λ sich als ganze Funktion der c_λ darstellen lässt.

§ 4. Wir beweisen diesen Hauptsatz der Theorie symmetrischer Funktionen derart, dass wir ihn für die einzelnen in § 2 charakterisierten Bildungstypen nachweisen, wobei sich gleichzeitig auch die Methode der Überführung einer symmetrischen Funktion der x_λ in eine Funktion der c_λ ergeben wird.

Wir beginnen mit denjenigen Typen, die nur eine Wurzel in jedem Summanden enthalten, d. h. mit den Formen $S(x_1^\lambda)$; eine solche Funktion ist die Summe der λ^{ten} Potenzen aller Wurzeln; wir führen die Bezeichnung

$$s_\lambda = S(x_1^\lambda)$$

ein. Dann ist es leicht, eine Rekursionsformel für die s_λ zu finden, falls $\lambda \geqq n$ ist.*

Die im vorigen Paragraphen aufgestellte Gleichung 4)

$$x^n - c_1 x^{n-1} + c_2 x^{n-2} - \ldots \pm c_n = 0$$

hat die Wurzeln $x = x_1, x_2, x_3, \ldots x_n$, so dass für $\alpha = 1, 2, 3, \ldots n$ die Gleichheiten gelten

$$x_\alpha{}^{n+r} - c_1 x_\alpha{}^{n+r-1} + c_2 x_\alpha{}^{n+r-2} - \ldots \pm c_n x_\alpha{}^r = 0, \quad r \geqq 0.$$

Addiert man die n Gleichungen, welche zu demselben r und zu $\alpha = 1, 2, 3, \ldots n$ gehören, so entsteht

A) $$s_{n+r} - c_1 s_{n+r-1} + c_2 s_{n+r-2} - \ldots \pm c_n s_r = 0, \quad r \geqq 0,$$

wobei $s_0 = n$ zu setzen ist. Dies ist die Rekursionsformel, vermöge deren $s_m (m \geqq n)$ durch $s_{m-1}, s_{m-2}, \ldots s_{m-n}$ ausgedrückt wird.

Es fehlt die entsprechende Formel für $m < n$. Um diese abzuleiten, setzen wir, da $f(x_\alpha) = 0$ ist,

$$\frac{f(x)}{x - x_\alpha} \equiv \varphi_\alpha(x) \equiv \frac{f(x) - f(x_\alpha)}{x - x_\alpha} = \frac{x^n - x_\alpha{}^n}{x - x_\alpha} - c_1 \frac{x^{n-1} - x_\alpha{}^{n-1}}{x - x_\alpha} + c_2 \frac{x^{n-2} - x_\alpha{}^{n-2}}{x - x_\alpha} - \ldots$$
$$= (x^{n-1} + x^{n-2} x_\alpha + x^{n-3} x_\alpha{}^2 + \ldots) - c_1 (x^{n-2} + x^{n-3} x_\alpha + x^{n-4} x_\alpha{}^2 + \ldots) + \ldots$$
$$= x^{n-1} - d_1{}^{(\alpha)} x^{n-2} + d_2{}^{(\alpha)} x^{n-3} - d_3{}^{(\alpha)} x^{n-4} + \ldots,$$

wo demnach der Koefficient

$$d_\mu{}^{(\alpha)} = c_\mu - c_{\mu-1} x_\alpha + c_{\mu-2} x_\alpha{}^2 - c_{\mu-3} x_\alpha{}^3 + \ldots + (-1)^\mu x_\alpha{}^\mu$$

wird. Addiert man also die n Ausdrücke $d'_\mu, d''_\mu, \ldots d_\mu{}^{(\alpha)}, \ldots d_\mu{}^{(n)}$, so erhält die Summe $d'_\mu + d''_\mu + \ldots + d_\mu{}^{(\alpha)} + \ldots + d_\mu{}^{(n)}$ den Wert

5) $$c_\mu s_0 - c_{\mu-1} s_1 + c_{\mu-2} s_2 - \ldots + (-1)^\mu s_\mu$$

für alle Werte $\mu = 1, 2, 3, \ldots n-1$. Anderseits ist $d_\mu{}^{(\alpha)}$ als Koefficient von $x^{n-\mu-1}$ in der ganzen Funktion

$$\frac{f(x)}{x - x_\alpha} \equiv (x - x_1)(x - x_2) \ldots (x - x_{\alpha-1})(x - x_{\alpha+1}) \ldots (x - x_n)$$

gleich der Summe aller Produkte von je μ Elementen, welche aus der Reihe

$$x_1, x_2, \ldots x_{\alpha-1}, x_{\alpha+1}, \ldots x_n$$

herausgegriffen werden können. Die Anzahl dieser Produkte ist gleich

$$\frac{(n-1)(n-2)\ldots(n-\mu)}{1.2\ldots\mu};$$

die Anzahl aller in der Summe $d'_\mu + d''_\mu + \ldots d_\mu{}^{(n)}$ vorkommenden Produkte von je μ Elementen daher gleich

$$n \frac{(n-1)(n-2)\ldots(n-\mu)}{1.2\ldots\mu} = \frac{n(n-1)(n-2)\ldots(n-\mu+1)}{1.2.3\ldots\mu} \cdot (n-\mu).$$

* Euler: Opuscula varii argum. Demonstr. genuina theor. Newtoniani II, p. 108.

Diese Summe $d'_\mu + d''_\mu + \ldots + d_\mu^{(n)}$ ist ihrer Bildung nach symmetrisch in den Elementen $x_1, x_2, \ldots x_n$; alle ihre Summanden sind von gleichem Typus, nämlich gleich einem der $\frac{n(n-1)(n-2)\ldots(n-\mu+1)}{1.2.3\ldots\mu}$ Glieder von c_μ; jedes dieser Glieder kommt also, wie sich aus der Vergleichung der Anzahlen ergiebt, $(n-\mu)$-mal vor, d. h. es ist zu setzen

$$d'_\mu + d''_\mu + \ldots + d_\mu^{(n)} = (n-\mu)\, c_\mu,$$

und daher erhält man durch Verbindung dieses Resultates mit 5)

$$c_\mu s_0 - c_{\mu-1} s_1 + c_{\mu-2} s_2 - \ldots + (-1)^\mu s_\mu = (n-\mu)\, c_\mu.$$

Da $s_0 = n$ ist, so liefert diese Gleichung die gewünschte Rekursionsformel

B) $$s_\mu - c_1 s_{\mu-1} + c_2 s_{\mu-2} - \ldots + (-1)^\mu . \mu c_\mu = 0 \quad (\mu < n).$$

Diese Reihe von Gleichungen in Verbindung mit A) löst das aufgestellte Problem. Ausgeführt lauten die Gleichungen B) folgendermassen

$$B_1) \quad \begin{cases} s_0 - n = 0, \\ s_1 - c_1 = 0, \\ s_2 - c_1 s_1 + 2c_2 = 0, \\ s_3 - c_1 s_2 + c_2 s_1 - 3c_3 = 0, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ s_{n-1} - c_1 s_{n-2} + c_2 s_{n-3} - \ldots + (-1)^{n-1} n c_{n-1} = 0. \end{cases}$$

An diese Gleichungen schliessen sich dann diejenigen von A) an.*

§ 5. Die Auflösung der Formeln A), B) liefert die Darstellung von s_m durch die $c_1, c_2, \ldots c_n$. Es kann dies leicht durch Determinanten geschehen. Hier mögen wenigstens die ersten fertigen Formeln Platz finden**

$$C) \quad \begin{cases} s_0 = n, \\ s_1 = c_1, \\ s_2 = c_1^2 - 2c_2, \\ s_3 = c_1^3 - 3c_1 c_2 + 3c_3, \\ s_4 = c_1^4 - 4c_1^2 c_2 + 4c_1 c_3 + 2c_2^2 - 4c_4, \\ s_5 = c_1^5 - 5c_1^3 c_2 + 5c_1^2 c_3 + 5c_1 c_2^2 - 5c_1 c_4 - 5c_2 c_3 + 5c_5. \end{cases}$$

Dabei ist zu bemerken, dass z. B. für $n = 4$ alle c_λ, deren Index λ grösser als vier ist, gleich Null gesetzt werden müssen; dies sieht man direkt ein oder man leitet es auch daraus ab, dass man zu den gegebenen vier Elementen x_1, x_2, x_3, x_4 noch beliebig viele andere

* Die Formeln A), B) sind zuerst von Newton: arithm. univers. De transmutatione aequationum gegeben.

** Vergl. Faà di Bruno: Binäre Formen; deutsch bearb. von Walter, I § 1.

mit den Zahlenwerten Null hinzunimmt; denn hierdurch werden die Potenzsummen in keiner Weise geändert, während die c_5, c_6, ... sämtlich zu Null werden.

§ 6. Nachdem diese Fundamentalaufgabe gelöst ist, gehen wir zur Darstellung symmetrischer Funktionen von der Form $S(x_1^{\alpha}x_2^{\beta})$ durch die elementaren symmetrischen Funktionen c_1, c_2, ... c_n der x_λ über. Wir setzen zuerst voraus, dass α von β verschieden sei. Wenn man das Produkt der beiden Ausdrücke

$$s_\alpha = x_1^{\alpha} + x_2^{\alpha} + x_3^{\alpha} + \ldots + x_n^{\alpha},$$
$$s_\beta = x_1^{\beta} + x_2^{\beta} + x_3^{\beta} + \ldots + x_n^{\beta}$$

bildet, so erhält man auf der linken Seite $s_\alpha s_\beta$. Rechts kann man die Multiplikation derart durchführen, dass man zuerst je zwei untereinander stehende Glieder vereinigt und dann die übrigen Produkte ausrechnet. Das erstere Verfahren giebt $s_{\alpha+\beta}$; die zweite Operation liefert $S(x_1^{\alpha}x_2^{\beta})$. Denn erstens gehören alle entstehenden Produkte der Form $x_i^{\alpha}x_k^{\beta}$ an, zweitens kommt jedes Glied der symmetrischen Funktion $S(x_1^{\alpha}x_2^{\beta})$ wirklich vor und drittens tritt es auch nur einmal auf. Daher ist

$$6) \qquad S(x_1^{\alpha}x_2^{\beta}) = s_\alpha s_\beta - s_{\alpha+\beta} \quad (\alpha \gtrless \beta).$$

Ist ferner $\alpha = \beta$, so ändert sich bei der Multiplikation links gar nichts; an Stelle von $s_\alpha . s_\beta$ tritt nur s_α^2. Rechts geht $s_{\alpha+\beta}$ in $s_{2\alpha}$ über, so dass auch dabei keine Änderung auftritt. Dagegen gehen von den übrigen Gliedern je zwei, die vorher verschieden waren, in ein einziges über, nämlich $x_1^{\alpha}x_2^{\beta}$ und $x_1^{\beta}x_2^{\alpha}$, jedes in $x_1^{\alpha}x_2^{\alpha}$; es wird also aus $S(x_1^{\alpha}x_2^{\beta})$ für $\alpha = \beta$ entstehen $2S(x_1^{\alpha}x_2^{\alpha})$, und man erhält folglich für gleiche Exponenten

$$7) \qquad S(x_1^{\alpha}x_2^{\alpha}) = \tfrac{1}{2}(s_\alpha^2 - s_{2\alpha}).$$

§ 7. Zur Berechnung der symmetrischen ganzen Funktionen vom Typus $x_1^{\alpha}x_2^{\beta}x_3^{\gamma}$ benutzen wir die drei Reihen

$$s_\alpha = x_1^{\alpha} + x_2^{\alpha} + \ldots + x_n^{\alpha},$$
$$s_\beta = x_1^{\beta} + x_2^{\beta} + \ldots + x_n^{\beta},$$
$$s_\gamma = x_1^{\gamma} + x_2^{\gamma} + \ldots + x_n^{\gamma}.$$

Es seien zuerst die drei Indices α, β, γ unter einander verschieden. Das Produkt der linken Seite liefert $s_\alpha . s_\beta . s_\gamma$. Rechts multipliziert man zuerst je drei unter einander stehende Summanden; dies liefert $s_{\alpha+\beta+\gamma}$. Dann multipliziert man je zwei einer Kolonne angehörige Glieder mit einem dritten zu einer anderen Kolonne gehörigen; dies liefert die drei symmetrischen Funktionen $S(x_1^{\alpha+\beta}x_2^{\gamma})$,

$S(x_1^{\beta+\gamma}x_2^{\alpha})$, $S(x_1^{\gamma+\alpha}x_2^{\beta})$. Nimmt man endlich die noch übrigen, also nur Glieder zusammen, welche verschiedenen Kolonnen angehören, so erhält man die symmetrische Funktion $S(x_1^{\alpha}x_2^{\beta}x_3^{\gamma})$. Es wird demnach mit Hilfe der Resultate des vorigen Paragraphen

$$s_\alpha s_\beta s_\gamma = s_{\alpha+\beta+\gamma} + (s_{\alpha+\beta}s_\gamma - s_{\alpha+\beta+\gamma}) + (s_{\alpha+\gamma}s_\beta - s_{\alpha+\beta+\gamma}) + (s_{\beta+\gamma}s_\alpha - s_{\alpha+\beta+\gamma}) + S(x_1^{\alpha}x_2^{\beta}x_3^{\gamma})$$
$$= -2s_{\alpha+\beta+\gamma} + (s_{\alpha+\beta}s_\gamma + s_{\beta+\gamma}s_\alpha + s_{\gamma+\alpha}s_\beta) + S(x_1^{\alpha}x_2^{\beta}x_3^{\gamma});$$

$$8)\quad S(x_1^{\alpha}x_2^{\beta}x_3^{\gamma}) = s_\alpha s_\beta s_\gamma - (s_{\alpha+\beta}s_\gamma + s_{\beta+\gamma}s_\alpha + s_{\gamma+\alpha}s_\beta) + 2s_{\alpha+\beta+\gamma}.$$

Wären zwei der Indices, z. B. α und β, einander gleich, so würde rechts in der letzten Gleichung 8) keine wesentliche Änderung eintreten; dagegen würde links wieder

$$[S(x_1^{\alpha}x_2^{\beta}x_3^{\gamma})]_{\alpha=\beta} = 2S(x_1^{\alpha}x_2^{\alpha}x_3^{\gamma})$$

gesetzt werden müssen, da je zwei Glieder $x_1^{\alpha}x_2^{\beta}x_3^{\gamma}$ und $x_1^{\beta}x_2^{\alpha}x_3^{\gamma}$ für $\alpha=\beta$ in ein und dasselbe Glied $x_1^{\alpha}x_2^{\alpha}x_3^{\gamma}$ übergehen. Ebenso würden sich für $\alpha=\beta=\gamma$ je $6=1.2.3$ Glieder der Form $x_1^{\alpha}x_2^{\beta}x_3^{\gamma}$, welche im allgemeinen Falle von einander verschieden sind, zu einem einzigen vereinigen, so dass man hätte

$$[S(x_1^{\alpha}x_2^{\beta}x_3^{\gamma})]_{\alpha=\beta=\gamma} = 3!\,S(x_1^{\alpha}x_2^{\alpha}x_3^{\alpha}).$$

Demnach entstehen die beiden speziellen Formeln

$$9)\quad S(x_1^{\alpha}x_2^{\alpha}x_3^{\beta}) = \tfrac{1}{2}(s_\alpha^{\,2}s_\beta - s_{2\alpha}s_\beta - 2s_\alpha s_{\alpha+\beta} + 2s_{2\alpha+\beta}),$$

$$10)\quad S(x_1^{\alpha}x_2^{\alpha}x_3^{\alpha}) = \tfrac{1}{6}(s_\alpha^{\,3} - 3s_{2\alpha}s_\alpha + 2s_{3\alpha}).$$

§ 8. Da die bisher befolgte Methode in gleicher Weise auf Typen von symmetrischen Funktionen angewendet werden kann, bei denen in jedem Gliede mehr als drei Elemente x_λ auftreten, so erkennt man die Reduktion der höheren auf niedere Formen; und da eine jede symmetrische Funktion in solche Typen zerlegt werden kann, so folgt:

Lehrsatz II. Jede ganze symmetrische Funktion der Grössen x_1, x_2, $\ldots x_n$ lässt sich als ganze Funktion der Potenzsummen s_λ derselben Grössen und daher auch als ganze Funktion der elementaren symmetrischen Funktionen c_1, c_2, $\ldots c_n$ ausdrücken.

Es muss jetzt noch der wichtige Zusatz bewiesen werden, dass eine solche Darstellung einer symmetrischen Funktion nur auf eine einzige Art möglich ist.

§ 9. Um diesen Nachweis zu liefern, nennen wir den Term

$$x_1^{m_1}x_2^{m_2}x_3^{m_3}\ldots \text{ höher als } x_1^{\mu_1}x_2^{\mu_2}x_3^{\mu_3}\ldots,$$

wenn die erste der Differenzen

$$m_1 - \mu_1, \quad m_2 - \mu_2, \quad m_3 - \mu_3, \quad \ldots,$$

welche nicht verschwindet, einen positiven Wert hat. Man legt also bei dieser Bestimmung eine willkürliche Rangfolge der x zu Grunde.*

Dann enthalten

$$c_1, \; c_2, \; c_3, \; \ldots c_\lambda, \; \ldots$$

als höchste Terme die folgenden

$$x_1, \quad x_1 x_2, \quad x_1 x_2 x_3, \quad \ldots x_1 x_2 x_3 \ldots x_\lambda, \quad \ldots,$$

und es liefert die Funktion

$c_1^{\alpha} c_2^{\beta} c_3^{\gamma} \ldots$ als höchsten Term $x_1^{\alpha+\beta+\gamma+\cdots} . x_2^{\beta+\gamma+\cdots} . x_3^{\gamma+\cdots} \ldots$

Damit also die beiden höchsten Terme zweier Ausdrücke

$$C_\lambda c_1^{\alpha} c_2^{\beta} c_3^{\gamma} \ldots \text{ und } C_l c_1^{a} c_2^{b} c_3^{c} \ldots$$

einander gleich seien, muss

$$\ldots \gamma = c, \quad \beta = b, \quad \alpha = a; \quad C_\lambda = C_l$$

werden, d. h. zwei verschiedene Systeme von Exponenten bei $c_1, c_2 \ldots c_n$ liefern verschiedene höchste Terme.

Könnte nun eine ganze symmetrische Funktion von $x_1, x_2, \ldots x_n$ in zwei wesentlich verschiedene Funktionen von $c_1, c_2, \ldots c_n$ umgewandelt werden, so würde für alle Werte von $x_1, x_2, \ldots x_n$ die Gleichung

$$\varphi(c_1, c_2, \ldots c_n) = \psi(c_1, c_2, \ldots c_n)$$

bestehen; die Differenz $\varphi - \psi$, welche als Funktion der c_λ nicht identisch Null ist (denn sonst würde die Umwandlung nicht auf zwei verschiedene Arten vor sich gegangen sein), ist als Funktion der x_λ identisch Null.

Denkt man sich nun in $\varphi - \psi$ die etwa vorhandenen, sich gegenseitig zerstörenden Terme der $c_1, c_2 \ldots c_n$ getilgt und übersetzt die zurückbleibenden Glieder in eine Funktion der x, welche nach einer der Variablen x geordnet

$$f_1 x_\alpha^{r} + f_2 x_\alpha^{r-1} + \ldots$$

heissen möge, so wird dieser Ausdruck nicht identisch Null sein, da er einen aus $\varphi - \psi$ entspringenden höchsten, von Null verschiedenen Term enthält.

Es müsste demnach für jedes Spezialsystem von Werten für die x_λ

$$f_1 x_\alpha^{r} + f_2 x_\alpha^{r-1} + \ldots + f_{r+1} = 0$$

---

* Gauss: Demonstr. nova altera etc., § 5, Ges. W. III. S. 37—38. Vergl. L. Kronecker, Monatsber. d. Berl. Akad. 1880, S. 943 ff.

sein. Wählt man aber $r+1$ Systeme von Werten für die x_λ, welche sich nur durch die für x_α festgesetzten Werte unterscheiden, so erkennt man die Unmöglichkeit dieser Annahme, und es folgt:

Lehrsatz III. Eine ganze symmetrische Funktion von x_1, x_2, $\ldots x_n$ lässt sich nur auf Eine Art in eine ganze Funktion der elementaren symmetrischen Funktionen c_1, c_2, $\ldots c_n$ umsetzen.

§ 10. Die soeben gemachte Bemerkung, dass $c_1^{\alpha} c_2^{\beta} c_3^{\gamma} \ldots$ als höchsten Term $x_1^{\alpha+\beta+\gamma+\cdots} . x_2^{\beta+\gamma+\cdots} . x_3^{\gamma+\cdots} \ldots$ liefert, führt dazu, den literalen Teil einer gegebenen symmetrischen, homogenen ganzen Funktion der Dimension n sofort aufzustellen.*

Enthält nämlich die gegebene Funktion eine und daher jede der Variabeln höchstens in der Potenz m, so darf jeder Summand des Ausdrucks in den c_λ höchstens m Faktoren enthalten. Denn erstens liefern zwei verschiedene Terme $c_1^{\alpha} c_2^{\beta} c_3^{\gamma} \ldots$, $c_1^{\alpha'} c_2^{\beta'} c_3^{\gamma'} \ldots$ verschiedene höchste Terme, so dass diese sich nicht zerstören können; und zweitens liefert $c_1^{\alpha} c_2^{\beta} c_3^{\gamma} \ldots$ die Potenz $x_1^{\alpha+\beta+\gamma+\cdots}$, so dass $\alpha+\beta+\gamma \ldots \leqq m$ sein muss.

Ferner wird die Dimension von $x_1^{\alpha+\beta+\gamma+\cdots} . x_2^{\beta+\gamma+\cdots} . x_3^{\gamma+\cdots} \ldots$ gleich $\alpha+2\beta+3\gamma+\ldots$; da der betrachtete Ausdruck ein homogener ist, muss bei dem entsprechenden Gliede, nämlich bei $c_1^{\alpha} c_2^{\beta} c_3^{\gamma} \ldots$ die Summe $\alpha+2\beta+3\gamma+\ldots$ gleich der Dimension n der homogenen symmetrischen Funktion sein. Durch diese beiden Beschränkungen, welche den Exponenten der c auferlegt sind, nämlich:

$$\alpha+\beta+\gamma \ldots \leqq m, \quad \alpha+2\beta+3\gamma+\ldots = n$$

scheidet ein grosser Teil der möglichen Glieder aus. Sind also q_0, q_1, $\ldots$ noch unbekannte Konstante, so folgt z. B. für

$$S(x_1^2 x_2^2 x_3^2 x_4) = q_0 c_7 + q_1 c_1 c_6 + q_2 c_2 c_5 + q_3 c_3 c_4 \quad (m=2, n=7)$$

und für

$$S[(x_1-x_2)^2 (x_2-x_3)^2 (x_3-x_1)^2] = q_0 c_6 + q_1 c_1 c_5 + q_2 c_2 c_4 + q_3 c_3^2 + q_4 c_1^2 c_4 + q_5 c_1 c_2 c_3 + q_6 c_2^3 + q_7 c_1^3 c_3 + q_8 c_1^2 c_2^2.$$

Die noch unbekannten numerischen Koefficienten werden dann am einfachsten durch Zahlenbeispiele berechnet. So erhält man im zweiten Falle für

I) $x_1=1$, $x_2=-1$, $x_3=x_4=\ldots=0$; $c_1=0$, $c_2=-1$, $c_3=c_4=\ldots=0$, $S=4=-q_6$; $q_6=-4$.

---

* Vergl. Salmon: Lessons introd. to the modern higher Algebra § 54. Kronecker: Monatsber. d. Berl. Akad. 1880, S. 943 ff.

II) $x_1=1,\ x_2=1,\ x_3=x_4=\ldots=0;\quad c_1=2,\ c_2=1,\ c_3=c_4=\ldots=0,$
$S=0=-4+4q_8;\quad q_8=1.$

III) $x_1=2,\ x_2=2,\ x_3=-1,\ x_4=\ldots=0;\quad c_1=3,\ c_2=0,\ c_3=-4,\ c_4=\ldots=0,$
$S=0=16q_3-4.27q_7;\quad 27q_7=4q_3.$

IV) $x_1=6,\ x_2=3,\ x_3=-1,\ x_4=\ldots=0;\quad c_1=7,\ c_2=0,\ c_3=-36,\ c_4=\ldots=0,$
$S=400=36q_3-7^3q_7;\quad q_3=-27;\quad q_7=-4.$

V) $x_1=1,\ x_2=1,\ x_3=1,\ x_4=\ldots=0;\quad c_1=3,\ c_2=3,\ c_3=1,\ c_4=\ldots=0,$
$S=0=-27+9q_5-108-108+81;\quad q_5=18.$

u. s. f.

Sind x_1, x_2, x_3 die einzigen vorkommenden Grössen, so geht die linke Seite in den Ausdruck $(x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2$ über, den wir mit Δ bezeichnen und „Diskriminante der Grössen x_1, x_2, x_3“ benennen. Die wesentlichsten Eigenschaften dieser Funktion sind die, dass sie symmetrisch ist und dass ihr Verschwinden für die Gleichheit zweier der drei Grössen x_1, x_2, x_3 hinreichend und notwendig ist. Rechts muss $c_4=c_5=c_6=0$ gesetzt werden und es entsteht daher die Gleichung

$$\Delta=-27c_3^2+18c_1c_2c_3-4c_2^3-4c_1^3c_3+c_1^2c_2^2.$$

§ 11. Allgemein können wir als die Diskriminante der n Grössen x_1, x_2, $\ldots x_n$ diejenige symmetrische Funktion der x_λ bezeichnen, deren Verschwinden für die Gleichheit zweier der n Grössen x_λ hinreichend und notwendig ist. Sie hat die Form

11) $$\Delta=\prod_{\lambda,\mu}(x_\lambda-x_\mu)^2 \qquad (\lambda<\mu;\ \lambda=1,2,\ldots n-1;\ \mu=2,3,\ldots n).$$
$$=(x_1-x_2)^2(x_1-x_3)^2(x_1-x_4)^2\ldots(x_1-x_n)^2$$
$$(x_2-x_3)^2(x_2-x_4)^2\ldots(x_2-x_n)^2$$
$$(x_3-x_4)^2\ldots(x_3-x_n)^2$$
$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot$$
$$(x_{n-1}-x_n)^2,$$

und enthält $\frac{n(n-1)}{2}$ Faktoren von der Form $(x_\lambda-x_\mu)^2$, $(\lambda<\mu)$; ihre Dimension ist $n(n-1)$; die höchste Potenz, in welcher jede Unbekannte x vorkommt, ist die $2(n-1)^{\text{te}}$; sie ist das Quadrat einer ganzen, nicht mehr symmetrischen Funktion der x_1, x_2, $\ldots x_n$, von welcher noch vielfach die Rede sein wird.

§ 12. Wir gehen zur Berechnung einer symmetrischen Funktion über, bei welcher die Diskriminante eine Rolle spielt. Die Gleichung, deren Wurzeln x_1, x_2, $\ldots x_n$ sind, heisse wie oben 3)

$$f(x)=0;$$

dann wird, wenn wir setzen

$$\frac{df(x)}{dx} = f'(x),$$

für alle Werte $\lambda = 1, 2, 3, \ldots n$ die Gleichung gelten

$$f'(x_\lambda) = (x_\lambda - x_1)(x_\lambda - x_2)\ldots(x_\lambda - x_{\lambda-1})(x_\lambda - x_{\lambda+1})\ldots(x_\lambda - x_n).$$

Wir bilden die symmetrische ganze Funktion

$$S[x_1^\alpha f'(x_2) f'(x_3)\ldots f'(x_n)];$$

diese enthält nur n solcher Summanden; jeder derselben ist durch $x_1 - x_2$ teilbar, da in jedem mindestens einer der beiden Faktoren $f'(x_1)$, $f'(x_2)$ auftritt; ja es sind alle Summanden, mit Ausnahme der beiden ersten, durch $(x_1 - x_2)^2$ teilbar, da jene anderen sämtlich $f'(x_1).f'(x_2)$ enthalten. Diese beiden ersten aber lauten zusammengenommen

$$x_1^\alpha f'(x_2) f'(x_3)\ldots f'(x_n) + x_2^\alpha f'(x_1) f'(x_3)\ldots f'(x_n)$$
$$= f'(x_3) f'(x_4)\ldots f'(x_n).(x_1 - x_2)\{x_1^\alpha(x_2 - x_3)(x_2 - x_4)\ldots - x_2^\alpha(x_1 - x_3)(x_1 - x_4)\ldots\}.$$

Diese Summe ist, weil ja die geschweifte Klammer für $x_1 = x_2$ zu Null wird, auch durch $(x_1 - x_2)^2$ teilbar. Es ist also $(x_1 - x_2)^2$ ein Faktor von S. Was von den beiden Wurzeln x_1, x_2 gilt, ist auch für jede andere Kombination x_λ, x_μ richtig. Es hat somit S den Faktor

$$\Delta = \prod_{\lambda,\mu}(x_\lambda - x_\mu)^2 \qquad (\lambda < \mu;\ \lambda = 1, 2, \ldots n-1;\ \mu = 2, 3, \ldots n),$$

d. h. S ist durch die Diskriminante von $f(x)$ teilbar, wo $f(x)$ als Repräsentantin der n Wurzeln x_1, x_2, $\ldots x_n$ eingesetzt ist. Nun ist

$$f'(x_1) \text{ nach } x_1 \text{ vom Grade } n-1,$$
$$f'(x_\lambda) \quad „ \quad x_1 \quad „ \quad „ \quad 1\,(\lambda \neq 1);^*$$

folglich ist

$$x_1^\alpha f'(x_2) f'(x_3)\ldots f'(x_n) \text{ nach } x_1 \text{ vom Grade } \alpha + n - 1,$$
$$x_\lambda^\alpha f'(x_1) f'(x_2)\ldots f'(x_n) \quad „ \quad x_1 \quad „ \quad „ \quad 2n-3$$

und, falls α geringer ist als $n-1$, wird

$$S \text{ nach } x_1 \text{ vom Grade } 2n-3.$$

Es ist aber

$$\Delta \quad „ \quad x_1 \quad „ \quad „ \quad 2n-2;$$

da Δ ein Teiler von S ist, so muss der andere Faktor Null sein, d. h. wir erhalten die Formel

$$S[x_1^\alpha f'(x_2) f'(x_3)\ldots f'(x_n)] = 0, \quad (\alpha < n-1.)$$

---

* Das Zeichen $\neq$ möge „ungleich“ bedeuten; es ist in vielen Fällen dem $\gtrless$ vorzuziehen, z. B. in allen, in welchen Grössenverhältnisse nicht auftreten.

Ohne Änderung des Beweises und des Resultats hätten wir für x_1^{α} eine beliebige Funktion des Grades α nehmen können; es sei $\varphi(x)$ eine solche, dann wird

$S[\varphi(x_1)f'(x_2)f'(x_3)\ldots f'(x_n)]=0$ (falls φ vom Grade $\alpha<n-1$ ist).

Die gewöhnliche Form, unter welcher die vorstehende Gleichung geschrieben wird, geht aus der eben erhaltenen durch Division mit

$$f'(x_1)f'(x_2)f'(x_3)\ldots f'(x_n)=(-1)^{\frac{n(n-1)}{2}}\Delta$$

hervor; sie lautet

D) $$\sum_{\lambda=1}^{n}\frac{\varphi(x_\lambda)}{f'(x_\lambda)}=0$$ (falls φ von geringerem Grade ist als f').

Ist α gleich $n-1$, so wird

$$S \text{ nach } x_1 \text{ vom Grade } 2n-2,$$
$$\Delta \quad \text{„} \quad x_1 \quad \text{„} \quad \text{„} \quad 2n-2,$$

und da Δ ein Faktor von S ist, so können beide Funktionen S und Δ sich nur durch einen von x_1 unabhängigen Faktor unterscheiden. Was für x_1 gilt, ist für jede der anderen Grössen x_λ richtig; also ist

$$S=\Delta.c,$$

wo c einen numerischen Faktor bezeichnet. Um diesen zu berechnen, beachten wir, dass nur der erste Summand in S nach x_1 vom Grade $2n-2$ wird, dass alle folgenden von niederen Graden sind, und dass der Koefficient von x_1^{2n-2} infolgedessen gleich

$$(-1)^{n-1}(x_2-x_3)(x_2-x_4)\ldots(x_2-x_n).(x_3-x_2)(x_3-x_4)\ldots(x_3-x_n)\ldots$$
$$\ldots(x_n-x_2)(x_n-x_3)\ldots(x_n-x_{n-1})$$
$$=(-1)^{\frac{n(n-1)}{2}}(x_2-x_3)^2(x_2-x_4)^2\ldots(x_2-x_n)^2.(x_3-x_4)^2\ldots(x_3-x_n)^2\ldots(x_{n-1}-x_n)^2$$

ist. In $c\Delta$ ist der Koefficient von x_1^{2n-2} gleich

$$c.(x_2-x_3)^2(x_2-x_4)^2\ldots(x_2-x_n)^2.(x_3-x_4)^2\ldots(x_3-x_n)^2\ldots(x_{n-1}-x_n)^2,$$

so dass sich ergiebt

$$c=(-1)^{\frac{n(n-1)}{2}}$$

und

$$S[x_1^{n-1}f'(x_2)f'(x_3)\ldots f'(x_n)]=(-1)^{\frac{n(n-1)}{2}}\Delta,$$

oder, ähnlich wie oben, durch Einführung der ganzen Funktion $\varphi(x)$

$$S[\varphi(x_1)f'(x_2)\ldots f'(x_n)]=(-1)^{\frac{n(n-1)}{2}}\Delta \text{ (falls } \varphi(x)=x^{n-1}+\alpha x^{n-2}+\ldots \text{ ist)}$$

E) $$\sum_{\lambda=1}^{n}\frac{\varphi(x_\lambda)}{f'(x_\lambda)}=1.$$*

* Die Formeln D), E) stammen von Euler: Calcul. integr. II § 1169.

§ 13. Ist eine aus den Elementen $x_1, x_2, \ldots x_n$ gebildete ganze Funktion nicht symmetrisch, so wird sie bei allen möglichen Vertauschungen der $x_1, \ldots x_n$ untereinander verschiedene Formen und also bei von einander völlig unabhängigen x auch verschiedene Werte annehmen. Die Ausführung einer derartigen Vertauschung oder Permutation der Elemente x_i untereinander soll Substitution heissen, so dass die Permutation das Resultat einer Thätigkeit, der Substitution ist.

Eine beliebige Substitution verändert die Form einer symmetrischen Funktion nicht; dagegen giebt es andere Funktionen, deren Formen durch Substitutionen geändert werden können; so nehmen

I) $x_1^2 - x_2^2 + x_3^2 - x_4^2, \quad x_1 x_2^2 x_3 + x_4 x_5 + x_6, \quad x_1^3 + x_1^2 + x_1$

bei gewissen Substitutionen andere Werte an, z. B. bei der Vertauschung von x_1 und x_2 die Werte:

II) $-x_1^2 + x_2^2 + x_3^2 - x_4^2, \quad x_1^2 x_2 x_3 + x_4 x_5 + x_6, \quad x_2^3 + x_2^2 + x_2.$

Die beiden ersten von diesen drei Funktionen I) bleiben für die Vertauschung von x_1 und x_3 ungeändert, die zweite ferner, wenn man x_4 und x_5 miteinander vertauscht u. s. w.

Je nach der Anzahl der Werte, welche eine ganze Funktion bei allen überhaupt möglichen Vertauschungen der Elemente annehmen kann, heisst dieselbe ein-, zwei-, drei-, vierwertig u. s. f. Die Existenz einwertiger Funktionen war ersichtlich; die Hauptsätze aus der Theorie derselben sind im ersten Teile dieses Kapitels besprochen worden.

Wir werfen jetzt die Frage nach der Existenz zweiwertiger Funktionen auf.

Angenommen, es gäbe zweiwertige Funktionen, so sei $\varphi(x_1, x_2 \ldots x_n)$ eine solche; ihre beiden Werte bezeichnen wir durch

$$\varphi_1(x_1, x_2, \ldots x_n) \quad \text{und} \quad \varphi_2(x_1, x_2, \ldots x_n).$$

Was für Substitutionen auch immer auf $\varphi(x_1, \ldots x_n)$ angewendet werden mögen, das Resultat wird φ_1 oder φ_2 sein; ebenso ensteht aus φ_1 oder φ_2 unter der Einwirkung einer Substitution immer wieder φ_1 oder φ_2. Wendet man auf φ_1 und auf φ_2 gleichzeitig dieselbe Substitution an, so wird die Einwirkung derselben auf φ_1 etwas anderes hervorrufen als auf φ_2; denn es ist

$$\alpha) \qquad \varphi_1(x_1, x_2, \ldots x_n) \neq \varphi_2(x_1, x_2, \ldots x_n),$$

und führt nun die Substitution x_1 in x_{i_1}, x_2 in x_{i_2}, $\ldots x_\alpha$ in x_{i_α}, $\ldots$ über, so wird auch im Resultate

$$\beta) \qquad \varphi_1(x_{i_1}, x_{i_2}, \ldots x_{i_n}) \begin{cases} = \\ \neq \end{cases} (\varphi_2(x_{i_1}, x_{i_2}, \ldots x_{i_n})$$

werden, denn die beiden linken Seiten von α) und β) unterscheiden sich nur durch die Bezeichnung der Argumente von einander, und ebenso die rechten Seiten.

Da nun $\varphi_1(x_{i_1}, x_{i_2}, \ldots x_{i_n})$ infolge der Zweiwertigkeit entweder gleich $\varphi_1(x_1, \ldots x_n)$ oder gleich $\varphi_2(x_1, \ldots x_n)$ ist, so wird $\varphi_2(x_{i_1}, x_{i_2}, \ldots x_{i_n})$ respektive gleich $\varphi_2(x_1, \ldots x_n)$ oder gleich $\varphi_1(x_1, \ldots x_n)$. Mit anderen Worten: Diejenigen Substitutionen, welche den einen Wert der zweiwertigen Funktion φ nicht ändern, ändern auch den anderen nicht; diejenigen Substitutionen, welche den einen Wert von φ in den anderen überführen, verwandeln diesen zweiten rückwärts in den ersten.

Bilden wir jetzt aus der angenommenen Funktion φ, über deren Existenz noch gar nichts feststeht, die Differenz ihrer beiden Werte

$$\psi_1 = \varphi_1 - \varphi_2,$$

so hat diese Funktion gleichfalls zwei und nur zwei Werte. Denn jede Substitution lässt entweder φ_1 und φ_2 ungeändert und damit auch ψ_1, oder sie verwandelt φ_1 in φ_2 und φ_2 in φ_1 und ruft dadurch den zweiten Wert

$$\psi_2 = \varphi_2 - \varphi_1 = -\psi_1$$

hervor. Existiert also eine zweiwertige Funktion φ, so existiert auch eine zweiwertige Funktion ψ, deren beide Werte sich nur durch ihre Vorzeichen von einander unterscheiden. Das Quadrat dieser Funktion ist daher symmetrisch. Eine solche Funktion heisse eine alternierende Funktion.

§ 14. Bleibt eine Funktion für jede Umsetzung von je zwei Elementen x_λ ungeändert, so bleibt sie überhaupt ungeändert, was für eine Substitution auch auf sie angewendet wird. Denn jede Substitution lässt sich aus einer Reihe von derartigen Umstellungen, die wir Transpositionen nennen wollen, zusammensetzen. Wir nehmen an, die Richtigkeit dieses Satzes sei für $n-1$ Elemente nachgewiesen; dann zeigen wir sie auch für n Elemente. Sollen $x_1, x_2, x_3, \ldots x_n$ durch $x_{i_1}, x_{i_2}, x_{i_3}, \ldots x_{i_n}$ ersetzt werden, wo die Zahlen $i_1, i_2, \ldots i_n$ eine Umstellung der Zahlen 1, 2, 3, $\ldots n$ bedeuten, so führe man zuerst die Transposition aus, welche x_1 und x_{i_1} vertauscht; dadurch geht $x_1, x_2, x_3, \ldots x_n$ in $x_{i_1}, x_{k_2}, x_{k_3}, \ldots x_{k_n}$ über, wo die k_α bis auf ein einziges k mit den α übereinstimmen, und

man hat dann nur noch die Überführung von $x_{i_1}, x_{k_2}, x_{k_3}, \ldots x_{k_n}$ in $x_{i_1}, x_{i_2}, x_{i_3}, \ldots x_{i_n}$ zu bewerkstelligen. Da das erste x in beiden Stellungen schon dasselbe ist, so ist nur noch $x_{k_2}, x_{k_3}, \ldots x_{k_n}$ in $x_{i_2}, x_{i_3}, \ldots x_{i_n}$ umzuwandeln, d. h. die Aufgabe ist auf die gleiche bei $n-1$ Elementen reduziert.

Für $n=2$ ist der Satz selbstverständlich. Folglich ist er allgemein bewiesen und wir sehen:

Lehrsatz IV. Jede Substitution kann durch eine Folge von Transpositionen ersetzt werden.

§ 15. Es giebt also mindestens eine Transposition, welche den Wert einer alternierenden Funktion ändert und ihn dadurch in den entgegengesetzt gleichen umwandelt. Diese Transposition möge x_α und x_β mit einander vertauschen. Dann wird bei der Funktion ψ des § 13 zu setzen sein

$$\psi(x_1, \ldots x_\alpha, \ldots x_\beta, \ldots x_n) = -\psi(x_1, \ldots x_\beta, \ldots x_\alpha, \ldots x_n).$$

Für $x_\alpha = x_\beta$ wird daher ψ gleich seinem entgegengesetzten Wert, d. h. gleich Null. Demnach wird

$$\psi(x_1, \ldots z, \ldots x_\beta, \ldots x_n) = 0,$$

als Gleichung für die Unbekannte z aufgefasst, die Wurzel $z = x_\beta$ haben; das Polynom ψ ist also durch $z - x_\beta$ teilbar; folglich hat

$$\psi(x_1, \ldots x_\alpha, \ldots x_\beta, \ldots x_n)$$

den Faktor $x_\alpha - x_\beta$ und die Funktion ψ^2 den Faktor $(x_\alpha - x_\beta)^2$.

Weil ferner ψ^2 nach § 13 symmetrisch ist, so enthält es alle Faktoren von der Form $(x_\alpha - x_\beta)^2$; dies wird durch die Unveränderlichkeit der Form einer symmetrischen Funktion bedingt. Nun war

$$\Delta = (x_1 - x_2)^2 \ldots (x_1 - x_n)^2 . (x_2 - x_3)^2 \ldots (x_2 - x_n)^2 \ldots$$

die Diskriminante der n Werte $x_1, x_2, \ldots x_n$; also haben wir den

Lehrsatz V. Jede alternierende Funktion ist durch $\sqrt{\Delta}$ teilbar.

§ 16. Über die Existenz alternierender Funktionen ist auch durch den letzten Satz noch nichts ausgesagt. Der folgende Lehrsatz giebt Aufschluss über diese Frage.

Lehrsatz VI. Die Quadratwurzel aus der Diskriminante der n Grössen $x_1, x_2, \ldots x_n$ ist eine alternierende Funktion dieser n Grössen.

Denn $(\sqrt{\Delta})^2$ ist symmetrisch in den x; $\sqrt{\Delta}$ hat also höchstens zwei Werte. Schreibt man

$$\sqrt{\Delta} = (x_1 - x_2)(x_1 - x_3)\ldots(x_1 - x_n)$$
$$(x_2 - x_3)\ldots(x_2 - x_n)$$
$$\ldots\ldots\ldots$$

und wendet die Transposition an, welche x_1 und x_2 mit einander vertauscht, so ändert der erste Faktor der ersten Zeile sein Vorzeichen; die übrigen Faktoren der ersten Zeile gehen in die darunter stehenden der zweiten über, und umgekehrt die der zweiten in die darüber stehenden der ersten Zeile, während in den übrigen Zeilen, welche weder x_1 noch x_2 enthalten, keine Änderung vor sich geht. Es wird also aus $\sqrt{\Delta}$ entstehen $-\sqrt{\Delta}$. Folglich hat $\sqrt{\Delta}$ mindestens zwei Werte.

$\sqrt{\Delta}$ ist also in der That zweiwertig.

§ 17. Lehrsatz VII. Jede alternierende ganze Funktion ist von der Form

$$S.\sqrt{\Delta},$$

wobei $\sqrt{\Delta}$ die Quadratwurzel aus der Diskriminante und S eine beliebige ganze symmetrische Funktion bedeuten.

Dass $S.\sqrt{\Delta}$ eine alternierende Funktion sei, erkennt man sofort. Ist umgekehrt ψ eine alternierende Funktion, so ist sie nach dem Lehrsatze V) durch $\sqrt{\Delta}$ teilbar. Es sei $(\sqrt{\Delta})^m$ die höchste als Faktor von ψ vorkommende Potenz von $\sqrt{\Delta}$. Dann wird der Quotient

$$12) \qquad \frac{\psi}{(\sqrt{\Delta})^m},$$

da in ihm Zähler wie Nenner höchstens ihr Zeichen ändern können, ein- oder zweiwertig sein. In letzterem Falle würde nach demselben Lehrsatze V) der Quotient gegen die Voraussetzung noch durch $\sqrt{\Delta}$ teilbar sein. 12) ist also symmetrisch und es folgt, wenn wir diesen Quotienten durch S_1 bezeichnen,

$$\psi = S_1(\sqrt{\Delta})^m.$$

Wäre m gerade, so wäre die rechte Seite und damit ψ selbst einwertig; es ist somit $m = 2n+1$, und da $(\sqrt{\Delta})^{2n} = \Delta^n$ also symmetrisch wird, so können wir diese Potenz zu S_1 ziehen und erhalten für $S_1\Delta^n = S$

$$\psi = S.\sqrt{\Delta}.$$

Zusatz. Aus der Form der alternierenden Funktionen folgt, dass sie bei einer beliebigen Substitution gleichzeitig mit $\sqrt{\Delta}$ ungeändert bleiben oder gleichzeitig mit $\sqrt{\Delta}$ ihr Vorzeichen ändern.

§ 18. Hiernach können wir jetzt die allgemeine Form zweiwertiger Funktionen finden. Ist φ eine solche Funktion, so wird die Summe ihrer beiden Werte $\varphi_1 + \varphi_2$ symmetrisch, die Differenz $\varphi_1 - \varphi_2$ derselben alternierend; wir können also setzen

$$\varphi_1 + \varphi_2 = 2S_1, \quad \varphi_1 - \varphi_2 = 2S_2\sqrt{\Delta}.$$

Hieraus folgt dann durch Addition und Subtraktion beider Gleichungen

$$\varphi_1 = S_1 + S_2\sqrt{\Delta}, \quad \varphi_2 = S_1 - S_2\sqrt{\Delta}, \quad \varphi = S_1 \pm S_2\sqrt{\Delta}.$$

Dass umgekehrt jede Funktion dieser Form zweiwertig ist, erkennt man ohne weiteres.

Lehrsatz VIII. Jede zweiwertige ganze Funktion hat die Form

$$\varphi = S_1 + S_2\sqrt{\Delta},$$

wobei S_1, S_2 ganze symmetrische Funktionen und $\sqrt{\Delta}$ die Quadratwurzel aus der Diskriminante bedeuten. Umgekehrt ist jede Funktion der angegebenen Form zweiwertig.

Zusatz. Jede ganze zweiwertige Funktion bleibt bei Substitutionen zugleich mit $\sqrt{\Delta}$ ungeändert oder sie ändert sich zugleich mit $\sqrt{\Delta}$.

§ 19. Aus den Zusätzen zu den beiden letzten Theoremen erkennt man, dass es von Wichtigkeit ist, die Substitutionen aufzufinden, welche den Wert von $\sqrt{\Delta}$ nicht ändern.

Von der Transposition, welche x_1 und x_2 vertauscht, wissen wir, dass sie $\sqrt{\Delta}$ ändert (§ 16). Ebensogut hätten wir aber das dortige Schema in anderer Weise anordnen können, so dass etwa x_α und x_β die Stellen von x_1 und x_2 einnehmen; nur wüssten wir dann nichts über die Bestimmung des Vorzeichens. Jedenfalls wird aber durch die Transposition, welche x_α und x_β untereinander vertauscht, einer der Werte von $\sqrt{\Delta}$ geändert; also nach § 13 auch der andere. Folglich wird $\sqrt{\Delta}$ bei Anwendung einer ganz beliebigen Transposition den entgegengesetzten Wert annehmen.

Dieses Resultat lässt sich leicht erweitern. Wendet man μ Transpositionen nacheinander auf $\sqrt{\Delta}$ an, so wird das Vorzeichen dieses Ausdrucks μ mal geändert; es tritt demnach zu $\sqrt{\Delta}$ der Faktor $(-1)^\mu$

hinzu. Ist μ gerade, so bleibt $\sqrt{\Delta}$ ungeändert; ist μ ungerade, so geht $\sqrt{\Delta}$ in $-\sqrt{\Delta}$ über. Gemäss § 14 Lehrsatz IV) können wir also sagen:

Lehrsatz IX. Alle Substitutionen, welche aus einer ungeraden Anzahl von Transpositionen gebildet werden können, ändern den Wert $\sqrt{\Delta}$ in $-\sqrt{\Delta}$ um; alle aus einer geraden Anzahl von Transpositionen gebildeten lassen $\sqrt{\Delta}$ ungeändert. Dasselbe findet bei jeder zweiwertigen Funktion statt.

Zusatz. Eine Substitution, die sich auf eine Art aus einer geraden respektive ungeraden Anzahl von Transpositionen zusammensetzen lässt, enthält bei jeder möglichen Zerlegung eine gerade respektive eine ungerade Anzahl von Transpositionen. Denn änderte sich dieser Charakter, so müsste dieselbe Substitution einmal $\sqrt{\Delta}$ ändern, einmal es ungeändert lassen. Dass bei der Zerlegung einer Substitution in Transpositionen grosse Willkürlichkeit herrscht, ist leicht einzusehen.

Wir kommen im nächsten Kapitel auf die durch den obigen Zusatz angeregten Fragen zurück.

§ 20. Lehrsatz X. Jede zweiwertige Funktion ist die Wurzel einer Gleichung zweiten Grades, deren Koefficienten rationale symmetrische Funktionen der Elemente $x_1, x_2, \ldots x_n$ sind.

Aus der in § 18 gefundenen Form

$$\varphi_1 = S_1 + S_2\sqrt{\Delta}, \quad \varphi_2 = S_1 - S_2\sqrt{\Delta}$$

folgt für die elementaren symmetrischen Funktionen von φ_1 und φ_2

$$\varphi_1 + \varphi_2 = 2S_1,$$
$$\varphi_1 \cdot \varphi_2 = S_1^2 - \Delta S_2^2;$$

beide Werte sind symmetrische Funktionen der Elemente. Wir erkennen, dass die Gleichung

$$\varphi^2 - 2S_1\varphi + (S_1^2 - \Delta S_2^2) = 0$$

die Wurzelwerte φ_1 und φ_2 liefert.

Zu bemerken ist hierbei, dass nicht umgekehrt jede quadratische Gleichung mit symmetrischen Funktionen zu Koefficienten auch zweiwertige Funktionen in unserem Sinne zu Wurzeln hat. Es ist dazu nötig, dass diese Wurzeln in den Elementen $x_1, x_2, \ldots x_n$ auch rational seien, was im allgemeinen nicht der Fall ist.

Zweites Kapitel.

Mehrwertige Funktionen und Substitutionengruppen.

§ 21. Es ist nach den Auseinandersetzungen des vorigen Kapitels möglich, den Gang unserer weiteren Untersuchungen wenigstens in allgemeinen Umrissen anzudeuten. Genau wie wir einwertige und zweiwertige Funktionen behandelt und die Substitutionen aufgesucht haben, welche die letztere Klasse von Funktionen ungeändert lassen, so wird es sich weiter darum handeln, die Existenz von Funktionen mit vorgeschriebener Wertezahl darzuthun oder als unmöglich nachzuweisen; die algebraische Form dieser Funktionen zu studieren; den Komplex aller derjenigen Substitutionen kennen zu lernen, welche eine vorliegende mehrwertige Funktion ungeändert lassen; die Beziehungen aller Werte dieser Funktion zu einander aufzusuchen. Weiter wird es sich darum handeln, die mehrwertigen Funktionen zu klassifizieren; sie — vielleicht, wie die zweiwertigen — als Wurzeln von Gleichungen mit symmetrischen Funktionen der Elemente als Koefficienten darzustellen; die Beziehungen zwischen Funktionen zu entdecken, welche für dieselben Substitutionen ihren Wert nicht ändern u. dergl. m.

§ 22. Zuerst muss eine expedite Schreibweise für Substitutionen ausfindig gemacht werden. — Wir betrachten eine rationale ganze Funktion der n von einander unabhängigen Grössen $x_1, x_2, \ldots x_n$; diese möge mit $\varphi(x_1, x_2, \ldots x_n)$ bezeichnet werden. Ändert man in diesem Ausdrucke die Stellungen der Elemente x_λ derart ab, dass man in φ für

$$x_1, x_2, \ldots x_n \quad \text{respektive setzt} \quad x_{i_1}, x_{i_2}, \ldots x_{i_n},$$

wobei der Komplex $i_1, i_2, \ldots i_n$ eine beliebige Permutation der Zahlen $1, 2, \ldots n$ bezeichnet, so erhält man aus der ursprünglichen Funktion

$$\varphi(x_1, x_2, \ldots x_n) \quad \text{den Ausdruck} \quad \varphi(x_{i_1}, x_{i_2}, \ldots x_{i_n}).$$

Wir betrachten die Art der Darstellung eines solchen Überganges von $x_1, x_2, \ldots x_n$ zu $x_{i_1}, x_{i_2}, \ldots x_{i_n}$; wir haben ihn im vorigen Kapitel bereits mit dem Namen einer Substitution belegt.

A. Erstens kann man denselben durch das Symbol

$$\begin{pmatrix} x_1, & x_2, & x_3, & \ldots & x_n \\ x_{i_1}, & x_{i_2}, & x_{i_3}, & \ldots & x_{i_n} \end{pmatrix}$$

bezeichnen; es mag dies andeuten, dass ein jedes Element der ersten Zeile durch das darunterstehende der zweiten ersetzt werden soll. Unbeschadet der Vollständigkeit der Darstellung können dabei alle

diejenigen Elemente, welche durch die Substitution nicht berührt werden, in dieser Darstellung weggelassen werden, alle diejenigen also, für welche $x_k = x_{i_k}$ ist. Freilich müsste dann die Zahl der Elemente von vornherein bekannt sein, ebenso wie dies bei φ selbst statthaben muss, indem z. B. aus der Form

$$\varphi = x_1 x_2 + x_3 x_4$$

noch durchaus nicht ersichtlich ist, ob nicht etwa noch Elemente $x_5, x_6, \ldots$ der Betrachtung zu Grunde liegen.

B. Zweitens kann man von den Resultaten des vorigen Kapitels Gebrauch machen: Jede Substitution kann in eine Reihe von Transpositionen zerlegt werden. Bezeichnen wir eine solche Transposition, d. h. die Umstellung zweier Elemente untereinander dadurch, dass beide in eine Klammer geschlossen werden, so wird jede Substitution als eine Folge

$$(x_a x_b)(x_c x_d)\ldots(x_p x_q)\ldots$$

dargestellt werden. Dabei kann die Zerlegung auf die mannigfaltigste Art vor sich gehen. Denn wir können, wie in § 14 des vorigen Kapitels gezeigt worden ist, zuerst durch eine Transposition ein ganz beliebiges Element an seine richtige Stelle bringen und dann mit den noch umzustellenden $n-1$ Elementen in gleicher Weise fortfahren. Ja wir können hierbei auch eine ganz willkürliche Transposition einschieben und deren Wirkung dann durch eine oder mehrere nicht unmittelbar folgende Transposition wieder zerstören.

C. Drittens kann man jede Substitution auch in der Form

$$(x_{a_1} x_{a_2} x_{a_3} \ldots x_{a_k})(x_{b_1} x_{b_2} \ldots x_{b_m})(x_{c_1} x_{c_2} \ldots x_{c_n})\ldots$$

darstellen. Die Bedeutung einer der aufgeschriebenen Klammern ist folgende: Jedes der in ihr vorkommenden Elemente mit Ausnahme des letzten wird durch das folgende, das letzte aber durch das erste derselben Klammer ersetzt. Man denkt sich die Klammern also cyklisch geschlossen, z. B. so, dass alle Elemente derselben aufeinander folgend auf der Peripherie eines Kreises angeordnet sind. Will man von der Darstellung in A) zu der jetzigen übergehen, so würden die Cykel lauten:

$$(x_1 x_{i_1} x_{i_{i_1}} \ldots)(x_a x_{i_a} x_{i_{i_a}} \ldots)\ldots$$

Auch hier ist es klar, dass die Elemente, welche von der Substitution nicht berührt werden, die also für sich allein je einen Cyklus bilden würden, fortgelassen werden können. Es sind dies dieselben, welche in der ersten Darstellung gleich den unter ihnen stehenden Elementen sind.

Die Klammern, in welche auf diese Art die Substitutionen zerlegt werden, sollen Cyklen heissen.

Eine vierte Darstellungsart, welche sich bei vielen wichtigen Spezialfällen als unentbehrlich ausweist, wird später besprochen werden.

§ 23. Es ist ersichtlich, dass in jeder dieser drei Darstellungsweisen A), B), C) etwas Willkürliches liegt. Bei A) ist die Anordnung der Elemente in der ersten Zeile ganz in unser Belieben gestellt; bei B) kann, wie wir gezeigt haben, die Art der Zerfällung in Transpositionen sehr verschieden sein; bei C) ist einmal die Aufeinanderfolge der Cyklen und zweitens das Anfangsglied jedes einzelnen Cyklus willkürlich.

Die erste dieser drei Darstellungsweisen leidet trotz ihrer scheinbaren Einfachheit doch an Unübersichtlichkeit; die zweite daran, dass ein und dasselbe Element beliebig oft in die Darstellung eintritt, so dass die wichtigste Frage: „durch welches Element wird ein gegebenes ersetzt?“ nicht auf den ersten Blick entschieden werden kann, und dass die Gleichheit zweier Substitutionen nicht sofort durch ihre Darstellung klargelegt wird.

Wir werden daher in den folgenden Untersuchungen fast ausschliesslich die Darstellung durch Cyklen verwenden.

Als Beispiel für das Auseinandergesetzte mag für $n = 7$ folgende Substitution dienen:

Die Folge $x_1, x_2, x_3, x_4, x_5, x_6, x_7$ soll durch $x_3, x_7, x_5, x_4, x_1, x_6, x_2$ ersetzt werden.

Die erste Methode liefert

$$\begin{pmatrix} x_1 x_2 x_3 x_4 x_5 x_6 x_7 \\ x_3 x_7 x_5 x_4 x_1 x_6 x_2 \end{pmatrix} = \begin{pmatrix} x_1 x_2 x_3 x_5 x_7 \\ x_3 x_7 x_5 x_1 x_2 \end{pmatrix};$$

nach der zweiten findet man für die Substitution

$$(x_1 x_3)(x_1 x_5)(x_2 x_7) = (x_1 x_3)(x_1 x_5)(x_1 x_2)(x_1 x_7)(x_1 x_2)$$
$$= (x_3 x_4)(x_5 x_6)(x_1 x_7)(x_3 x_7)(x_1 x_6)(x_2 x_7)(x_4 x_5)(x_2 x_4)(x_2 x_6) = \ldots$$

Da wir hier die Zerlegung in 3, 5 und 9 Transpositionen, also jedesmal in eine ungerade Anzahl besitzen, so ist dies zugleich ein Beispiel für Kapitel 1 § 19 Zusatz, und lehrt, dass $\sqrt{\Delta}$ für die hier betrachtete Substitution ihr Zeichen ändert.

Die dritte Methode liefert

$$(x_1 x_3 x_5)(x_2 x_7)(x_4)(x_6) = (x_1 x_3 x_5)(x_2 x_7) = (x_2 x_7)(x_3 x_5 x_1)$$
$$= (x_7 x_2)(x_5 x_1 x_3) = \ldots$$

§ 24. Wir suchen die Anzahl aller möglichen Substitutionen auf, indem wir diejenige aller möglichen Permutationen bestimmen.

Zwei Elemente x_1, x_2 können zwei verschiedene Permutationen bilden: $x_1 x_2$ und $x_2 x_1$. Kommt ein drittes Element zu diesen beiden,

so kann es bei jeder der vorhandenen beiden Permutationen an den Anfang treten: $x_3x_1x_2$, $x_3x_2x_1$, oder in die Mitte $x_1x_3x_2$, $x_2x_3x_1$, oder ans Ende: $x_1x_2x_3$, $x_2x_1x_3$. Es giebt also $2.3 = 3!$ Permutationen unter drei Elementen. Tritt ein viertes Element x_4 auf, so kann es bei jeder der vorhandenen 2.3 Permutationen an die erste, zweite, dritte oder vierte Stelle treten und dadurch aus jeder der vorhandenen 4 neue hervorrufen; es giebt also $2.3.4 = 4!$, ebenso bei 5 Elementen 5! Permutationen u. s. w., bei n Elementen $n!$ Permutationen.

Nimmt man nun für die erste Zeile in der Darstellungsweise A) der Substitutionen die natürliche Folge der Elemente $x_1, x_2, \ldots x_n$ und für die zweite Zeile der Reihe nach alle $n!$ möglichen Permutationen derselben, so erhält man alle möglichen von einander verschiedenen Substitutionen der n Elemente.

Zu bemerken ist, dass hierunter auch diejenige Substitution enthalten ist, bei der die erste und die zweite Zeile übereinstimmen. Diese stellt also gar kein Element um; sie werde mit 1 bezeichnet und als Einheit oder auch als identische Substitution angesehen.

Lehrsatz I. Für n Elemente giebt es $n!$ Substitutionen.

Um aus der Darstellungsweise B) dasselbe Resultat ableiten zu können, müssten eingehendere Untersuchungen gemacht werden, für welche hier nicht die Stelle ist; bei der Darstellungsweise C) ist es leicht, mit Hilfe der strengen Induction die Anzahl $n!$ festzustellen.

Man gelangt dabei zu einer Reihe interessanter Beziehungen, von denen wenigstens eine hier angegeben werden mag. Enthält eine Substitution, in deren Ausdruck alle Elemente aufgenommen werden

a Cyklen von α Elementen, b Cyklen von β Elementen, ...

$$\text{N)} \qquad a\alpha + b\beta + \ldots = n,$$

so lassen sich aus ihr durch Umstellung der Cyklen und durch Verschiebung der Elemente jedes einzelnen Cyklus

$$a!\alpha^a.b!\beta^b\ldots$$

Ausdrücke für dieselbe Substitution ableiten; folglich giebt es

$$\frac{n!}{a!\alpha^a.b!\beta^b\ldots}$$

von einander verschiedene Substitutionen, welche a Cyklen von α Elementen, b Cyklen von β Elementen u. s. f. besitzen. Summiert man in Hinsicht auf alle möglichen Zerlegungen N) der Zahl n, so erhält man alle möglichen $n!$ Substitutionen. Daher ist

$$\sum \frac{1}{a!\alpha^a.b!\beta^b\ldots} = 1.*$$

* Cauchy: Exercices d'analyse III, 173.

§ 25. Wendet man nun alle diese $n!$ Substitutionen auf $\varphi(x_1, \ldots x_n)$ an, d. h. führt man jede dieser Substitutionen, welche kurz mit

$$s_1 = 1,\ s_2,\ s_3, \ldots s_\alpha, \ldots s_{n!}$$

bezeichnet werden mögen, zwischen den $x_1, x_2, \ldots x_n$ in dem Ausdrucke φ durch, so erhält man, den durch die Substitution $s_1 = 1$ hervorgerufenen mitgerechnet, $n!$ Ausdrücke, welche mit

$$\varphi_{s_1} = \varphi_1 = \varphi,\quad \varphi_{s_2}, \varphi_{s_3}, \ldots \varphi_{s_\alpha}, \ldots \varphi_{s_{n!}};$$

oder wohl auch, wenn keine Verwechselung zu befürchten steht, mit

$$\varphi_1, \varphi_2, \varphi_3, \ldots \varphi_\alpha, \ldots \varphi_{n!}$$

bezeichnet werden mögen. Diese Werte brauchen nicht alle von einander verschieden zu sein; einige können den ursprünglichen Wert $\varphi(x_1, x_2, \ldots x_n)$ wieder annehmen. Auf den Komplex derjenigen Substitutionen, welche den Wert von φ nicht ändern, richten wir zunächst unsere Aufmerksamkeit. Ist φ symmetrisch, so wird dieser Komplex alle überhaupt vorhandenen Substitutionen umfassen; ist φ eine zweiwertige Funktion, so enthält er alle Substitutionen, welche aus einer geraden Anzahl von Transpositionen zusammengesetzt sind, und nur diese. — Sei ferner beispielshalber unter der Voraussetzung von nur vier Elementen x_1, x_2, x_3, x_4

$$\varphi(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4,$$

so wird dieser Wert für acht der überhaupt möglichen 24 Substitutionen ungeändert bleiben, nämlich für

$$s_1 = 1,\quad s_2 = (x_1x_2),\quad s_3 = (x_3x_4),\quad s_4 = (x_1x_2)(x_3x_4),$$
$$s_5 = (x_1x_3x_2x_4),\quad s_6 = (x_1x_4x_2x_3),\quad s_7 = (x_1x_3)(x_2x_4),\quad s_8 = (x_1x_4)(x_2x_3).$$

Für die übrigen $4! - 8 = 16$ Substitutionen ändert sich φ und zwar geht es entweder in

$$x_1x_3 + x_2x_4 \quad \text{oder in} \quad x_1x_4 + x_2x_3$$

über; wir lernen also, nebenbei bemerkt, hier eine dreiwertige Funktion von vier Elementen kennen, welche für acht von den 24 Substitutionen ihren Wert ungeändert beibehält.

§ 26. Alle diejenigen Substitutionen, welche eine Funktion $\varphi(x_1, x_2, \ldots x_n)$ ungeändert lassen, und deren Anzahl stets durch r bezeichnet werden wird, mögen

G) $$s_1 = 1,\ s_2,\ s_3, \ldots s_r$$

heissen; $s_1 = 1$ befindet sich natürlich unter ihnen. Nach der im vorigen Paragraphen eingeführten Bezeichnung ist dann

$$\varphi = \varphi_{s_1} = \varphi_{s_2} = \varphi_{s_3} = \ldots = \varphi_{s_r}.$$

Der Voraussetzung nach wird keine von $s_1, s_2, \dots s_r$ verschiedene Substitution s' den Wert φ ungeändert lassen; d. h. es ist stets

$$\varphi_{s'} \neq \varphi, \quad \text{wenn} \quad s' \neq s_\lambda \quad (\lambda = 1, 2, \dots r).$$

Wendet man jetzt auf φ zwei Substitutionen s_α, s_β unserer Reihe nach einander an und bezeichnet das Resultat, ähnlich wie oben bei einer einfachen Substitution, mit

$$\varphi_{s_\alpha s_\beta},$$

so wird, da $\varphi_{s_\alpha} = \varphi$ ist, das Resultat der beiden Operationen

$$\varphi_{s_\alpha s_\beta} = \varphi_{s_\beta} = \varphi$$

sein, und daraus lässt sich schliessen, dass $s_\alpha s_\beta$ auch in der obigen Reihe G) vorkommt: jede Substitution, welche durch die Aufeinanderfolge zweier der Substitutionen von G) hervorgerufen wird, befindet sich wiederum in der Reihe G). Was von zwei Substitutionen jener Reihe gilt, hat hiernach für beliebig viele gleichfalls Geltung.

Die aufeinander folgenden Anwendungen zweier oder mehrerer Substitutionen nennen wir das Produkt derselben und schreiben die Substitution σ, welche denselben Effekt auf φ ausübt, wie die Aufeinanderfolge von s_α und s_β, als Produkt $\sigma = s_\alpha s_\beta$. Es kommt das Produkt beliebig vieler s wieder unter der Reihe G) $s_1, s_2, s_3, \dots s_r$ vor. Die Operationenfolge in einem Produkte $\sigma = s_\alpha s_\beta s_\gamma \dots$ soll von links nach rechts gerechnet werden.

§ 27. Die Darstellung eines solchen Produktes von Substitutionen ergiebt sich in der von uns acceptierten Darstellungsweise durch Cyklen folgendermassen. Sind

$$s_\alpha = (x_a x_{a_1} x_{a_2} \dots)(x_{\mathfrak{a}} x_{\mathfrak{a}_1} x_{\mathfrak{a}_2} \dots) \dots, \quad s_\beta = (x_b x_{b_1} x_{b_2} \dots)(x_{\mathfrak{b}} x_{\mathfrak{b}_1} x_{\mathfrak{b}_2} \dots) \dots$$

die beiden Faktoren des zu bildenden Produktes, so wird in $s_\alpha s_\beta$ auf x_a dasjenige Element folgen, durch welches s_β das Element x_{a_1} ersetzt. Dies sei z. B. $x_{\mathfrak{a}_1}$; ferner wird in $s_\alpha s_\beta$ auf $x_{\mathfrak{a}_1}$ dasjenige Element folgen, durch welches s_β das Element $x_{\mathfrak{a}_2}$ ersetzt; dies sei z. B. $x_{\mathfrak{b}_2}$ u. s. w. Man erhält

$$s_\alpha s_\beta = (x_a x_{\mathfrak{a}_2} x_{\mathfrak{b}_2} \dots) \dots$$

Ist etwa die Substitution s_α so beschaffen, dass sie jeden Index g der Elemente $x_1, \dots x_g, \dots x_n$ durch i_g ersetzt; s_β derart, dass sie jeden Index g durch k_g ersetzt, oder in Formeln, ist:

$$s_\alpha = (x_1 x_{i_1} x_{i_{i_1}} \dots)(x_a x_{i_a} \dots), \quad s_\beta = (x_1 x_{k_1} x_{k_{k_1}} \dots)(x_b x_{k_b} \dots),$$

so wird das Produkt die Form haben

$$s_\alpha s_\beta = (x_1 x_{k_{i_1}} \dots)(x_s x_{k_{i_s}} \dots) \dots$$

Als Beispiel gelte

$$s_\alpha = (x_1 x_3 x_5)(x_2 x_7), \quad s_\beta = (x_2 x_4 x_6)(x_3 x_5),$$
$$s_\alpha s_\beta = (x_1 x_5)(x_2 x_7 x_4 x_6)(x_3) = (x_1 x_5)(x_2 x_7 x_4 x_6).$$

Wir haben hier den Ausdruck Produkt eingeführt. Es fragt sich, wie weit die fundamentalen algebraischen Multiplikationsregeln

$$a.b = b.a, \quad a.(b.c) = (a.b).c$$

verwendet werden dürfen. Die Untersuchung hierüber wird zeigen, dass das erste, das kommutative Gesetz im allgemeinen wegfällt, während das zweite, das associative bestehen bleibt.

In der That lehrt die obige Ausführung der Multiplikation von

$$s_\alpha = (x_1 x_{i_1} \ldots) \ldots, \quad s_\beta = (x_1 x_{k_1} \ldots) \ldots,$$

dass nur in dem Specialfalle, in welchem $i_{k_\alpha} = k_{i_\alpha}$ für jedes α ist, eine Faktorenvertauschung vorgenommen werden darf. Dies findet z. B. statt, wenn s_α und s_β keine gemeinsamen Elemente besitzen, wie sich beim ersten Anblick ergiebt.

Deshalb darf man die einzelnen Cyklen einer Substitution, welche ja keine gemeinsamen Elemente besitzen, ganz nach Belieben unter einander vertauschen. Bei der Darstellung B) S. 20 ist dies nicht möglich.

Ist dagegen, um zum associativen Gesetze überzugehen,

$$s_\alpha = \ldots (x_s x_{i_s} \ldots) \ldots, \quad s_\beta = \ldots (x_s x_{k_s} \ldots) \ldots, \quad x_\gamma = \ldots (x_s x_{l_s} \ldots) \ldots,$$

so folgt nachstehende Reihe von Produkten

$$s_\beta s_\gamma = \ldots (x_s x_{l_{k_s}} \ldots) \ldots, \quad s_\alpha s_\beta = \ldots (x_s x_{k_{i_s}} \ldots) \ldots,$$
$$s_\alpha (s_\beta s_\gamma) = \ldots (x_s x_{l_{k_{i_s}}} \ldots) \ldots, \quad (s_\alpha s_\beta) s_\gamma = \ldots (x_s x_{l_{k_{i_s}}} \ldots) \ldots,$$

und daraus der verlangte Satz.

Lehrsatz II. Bei der Multiplikation von Substitutionen ist eine Zusammenfassung der Faktoren in Unterprodukte ohne Änderung der Faktorenfolge gestattet. Eine Vertauschung der Faktoren liefert dagegen im allgemeinen verschiedene Resultate; erlaubt ist dieselbe, wenn die Faktoren keine gemeinsamen Elemente besitzen.

§ 28. Diejenigen Substitutionen

G) $$s_1 = 1, \; s_2, \; s_3, \; \ldots \; s_\alpha, \; \ldots \; s_r,$$

welche eine gegebene Funktion $\varphi(x_1, x_2, \ldots x_n)$ ungeändert lassen, bilden nach den vorstehenden Entwicklungen in der Hinsicht eine in sich geschlossene Gruppe, dass sich ihre Gesamtheit durch Multiplikation der einzelnen zugehörigen Substitutionen untereinander nicht ändert.

Mit diesem Namen einer Gruppe* soll stets ein Komplex von Substitutionen bezeichnet werden, welcher die gegebene charakteristische Eigenschaft der Reproduktion des Komplexes durch Multiplikation seiner Individuen besitzt. Die Anzahl der Elemente, um die es sich handelt, heisst der Grad der Gruppe. Es ist aber nicht nötig, dass alle Elemente auch wirklich in die Cyklen der Substitutionen eingehen. So bilden

$$s_1 = 1, \quad s_2 = (x_1 x_2)(x_3 x_4)$$

eine Gruppe, denn man hat $s_1 . s_2 = s_2 . s_1 = s_2$; $s_2 . s_2 = s_1 = 1$; diese Gruppe ist vom Grade 4, falls nur die Elemente x_1, x_2, x_3, x_4 der Betrachtung zu Grunde liegen. In weiterem Sinne kann aber diese Gruppe auch als solche von sechs Elementen $x_1, \ldots x_6$ gelten, wo dann allenfalls s_2 durch

$$s'_2 = (x_1 x_2)(x_3 x_4)(x_5)(x_6)$$

ersetzt werden könnte. Der Grad der Gruppe wäre dann gleich sechs.

Die Anzahl der Substitutionen einer Gruppe heisse ihre Ordnung; wie bereits oben gesagt, werde sie künftig stets mit dem Buchstaben r bezeichnet.

Der Komplex sämtlicher Substitutionen, welche den Wert von $\varphi(x_1, \ldots x_n)$ nicht ändern, heisse die zur Funktion φ gehörige Substitutionengruppe oder kürzer die Gruppe von φ. Der Grad derselben drückt die Anzahl der den Betrachtungen unterworfenen Grössen x_1, x_2, $\ldots x_n$ aus; die Ordnung der Gruppe giebt die Anzahl aller Substitutionen an, welche die Funktion φ nicht ändern.

Sind die vier Elemente x_1, x_2, x_3, x_4 gegeben, und ist

$$\varphi = x_1 x_2 + x_3 x_4,$$

so ist der Grad der zu φ gehörigen Gruppe gleich 4; ihre Ordnung ist, wie sich in § 25 zeigte, gleich 8.

Für die fünf Elemente x_1, x_2, $\ldots x_5$ wird dasselbe φ eine Gruppe vom Grade 5 und von der Ordnung 8 besitzen; sie ist mit der aus § 25 identisch.

Für die sechs Elemente x_1, x_2, $\ldots x_6$ wird dasselbe φ eine Gruppe vom Grade 6 besitzen. Zu der obigen Gruppe kommen hier noch alle diejenigen Substitutionen hinzu, welche x_5 und x_6 unter einander vertauschen, also zu den obigen acht noch folgende acht neue Substitutionen

* Cauchy, welcher in den Exercices d'analyse et de physique mathématique die erste systematische Darstellung der Substitutionentheorie gab, gebraucht den Ausdruck „System konjugierter Substitutionen“. Denselben behält Serret in seiner Algebra bei. Durch Galois ist die kürzere Bezeichnung „Gruppe“ eingeführt.

$s_9 = (x_5 x_6)$, $s_{10} = (x_1 x_2)(x_5 x_6)$, $s_{11} = (x_3 x_4)(x_5 x_6)$, $s_{12} = (x_1 x_2)(x_3 x_4)(x_5 x_6)$,
$s_{13} = (x_1 x_3 x_2 x_4)(x_5 x_6)$, $s_{14} = (x_1 x_4 x_2 x_3)(x_5 x_6)$, $s_{15} = (x_1 x_3)(x_2 x_4)(x_5 x_6)$,
$s_{16} = (x_1 x_4)(x_2 x_3)(x_5 x_6)$.

Die Ordnung der jetzt zu φ gehörigen Gruppe ist also $8 . 2 = 16$.

Es ist leicht zu sehen, dass, wenn man φ als von $n > 4$ Elementen abhängig ansieht, die Ordnung der zugehörigen Gruppe $8 . (n-4)!$ wird, und dass die Gruppe selbst erhalten wird, indem man die acht Substitutionen aus § 25 mit allen Substitutionen der Elemente x_5, x_6, $\ldots x_n$ multipliziert.

§ 29. Wir wollen, um den vollkommenen Zusammenhang zwischen mehrwertigen Funktionen und Substitutionengruppen nachzuweisen, jetzt ausser dem bereits gefundenen

Lehrsatz III. Für jede ein- oder mehrwertige Funktion giebt es eine Gruppe von Substitutionen, deren Anwendung auf die Funktion den Ausdruck derselben nicht ändert —

auch den umgekehrten Satz anführen und beweisen:

Lehrsatz IV. Für jede Gruppe von Substitutionen giebt es Funktionen, die für alle Substitutionen der Gruppe und auch nur für diese ungeändert bleiben.

Zuerst wollen wir eine Funktion der n von einander unabhängigen Grössen x_1, x_2, $\ldots x_n$ aufstellen, welche so viele verschiedene Werte haben soll, als überhaupt möglich sind, nämlich $n!$; φ soll also unter dem Einflusse jeder von der Einheit verschiedenen Substitution eine Wertabänderung erfahren.

Wir bilden mit $n+1$ beliebigen, von einander verschiedenen willkürlichen Konstanten α_0, α_1, $\ldots \alpha_n$ den linearen Ausdruck

$$\varphi = \alpha_0 + \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n .$$

Gäben die beiden Substitutionen $s_\alpha = \ldots (x_s x_{i_s} \ldots) \ldots$ und $s_\beta = \ldots (x_s x_{k_s} \ldots) \ldots$ bei ihrer Anwendung auf φ denselben Wert, so wäre

$$0 = \varphi_{s_\alpha} - \varphi_{s_\beta} = \alpha_1 (x_{i_1} - x_{k_1}) + \alpha_2 (x_{i_2} - x_{k_2}) + \ldots$$

Ordnet man diesen Ausdruck nach den x, so erhalte man

$$0 = (\alpha_{\iota_1} - \alpha_{\varkappa_1}) x_1 + (\alpha_{\iota_2} - \alpha_{\varkappa_2}) x_2 + \ldots ,$$

wo $\iota, \varkappa$ so bestimmt sind, dass $\lambda = \iota_{i_\lambda}$, $\mu = \varkappa_{k_\mu}$ für jedes $\lambda, \mu = 1, 2, \ldots n$ wird. Wegen der Unabhängigkeit der x von einander folgt, dass alle Klammern einzeln verschwinden müssen, also wegen der Willkürlichkeit der α, dass

$$\iota_\lambda = \varkappa_\lambda , \quad \text{folglich} \quad \iota_{i_\lambda} = \lambda = \varkappa_{k_\lambda} \quad \text{und} \quad \iota_{i_\lambda} = \varkappa_{i_\lambda} = \varkappa_{k_\lambda} ,$$

also

$$i_\lambda = k_\lambda \quad \text{und} \quad i = k$$

sein muss, so dass s_α mit s_β identisch wird. Nur in diesem Falle, d. h. wenn sie identisch sind, können zwei Substitutionen in ihrer Anwendung auf φ denselben Wert hervorrufen; φ hat demnach $n!$ Werte.

§ 30. Ist nun eine Substitutionengruppe G mit den Substitutionen

$$s_1 = 1,\ s_2,\ s_3,\ \ldots\ s_\alpha,\ \ldots\ s_r$$

gegeben, was wir symbolisch durch die Gleichung ausdrücken wollen:

$$G = [s_1, s_2, s_3, \ldots s_\alpha, \ldots s_r],$$

so bilden wir die $n!$-wertige lineare Funktion mit $(n+1)$ Parametern

$$\varphi_1 = \alpha_0 + \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n,$$

wenden auf dieselbe alle Substitutionen von G an und bezeichnen die Resultate dieser Operationen durch die an φ gesetzten Indices 1, s_2, $\ldots s_r$

$$\varphi_{s_1} = \varphi_1,\ \varphi_{s_2},\ \varphi_{s_3},\ \ldots\ \varphi_{s_r};$$

dann wird das Produkt derselben

$$\Phi = \varphi_{s_1} \cdot \varphi_{s_2} \cdot \varphi_{s_3} \ldots \varphi_{s_r}$$

eine der Funktionen sein, zu denen die Substitutionengruppe G gehört. Um dies nachzuweisen, muss gezeigt werden, 1) dass Φ für jede Substitution σ von G ungeändert bleibt; 2) dass Φ für jede Substitution τ, die nicht in G vorkommt, seinen Wert ändert. Was den ersten Punkt angeht, so hat man

$$\Phi_\sigma = \varphi_{s_1\sigma} \cdot \varphi_{s_2\sigma} \cdot \varphi_{s_3\sigma} \ldots \varphi_{s_r\sigma};$$

gemäss der Definition einer Gruppe sind $s_1\sigma = \sigma$, $s_2\sigma$, $s_3\sigma$, $\ldots\ s_r\sigma$ wieder in G enthalten. Diese Produkte sind aber auch sämtlich von einander verschieden; denn würden $s_\alpha\sigma$ und $s_\beta\sigma$ auf φ angewendet, denselben Effekt haben, so würde dies auch schon bei s_α und s_β der Fall und $s_\alpha = s_\beta$ sein. Also sind die Substitutionen

$$\sigma,\ s_2\sigma,\ s_3\sigma\ \ldots s_r\sigma \quad \text{mit den} \quad 1,\ s_2,\ s_3,\ \ldots\ s_r$$

bis auf die Reihenfolge identisch und daher ebenso die Funktionen

$$\varphi_\sigma,\ \varphi_{s_2\sigma},\ \ldots\ \varphi_{s_r\sigma} \quad \text{mit den} \quad \varphi_1,\ \varphi_{s_2},\ \ldots\ \varphi_{s_r},$$

und es ist demnach auch, wie behauptet wurde,

$$\Phi_\sigma = \Phi.$$

Was den zweiten Teil des Beweises angeht, so ist wegen der $n!$-Wertigkeit von φ der Wert φ_τ von allen Faktoren φ_1, φ_{s_2}, $\ldots\ \varphi_{s_r}$ verschieden, und zwar ist diese Verschiedenheit eine derartige, dass nicht etwa φ_τ gleich dem Produkte aus φ_{s_α} und einer Konstante c_α sein, und dann in

$$\varphi_\tau \varphi_{s_2\tau} \varphi_{s_3\tau} \ldots = c_1 \cdot c_2 \cdot c_3 \ldots \cdot \varphi_1 \cdot \varphi_{s_2} \cdot \varphi_{s_3} \ldots$$

wegen

$$c_1 c_2 c_3 \ldots = 1$$

gleichwohl das Produkt

$$\Phi_\tau = \Phi$$

sein kann. Denn wegen der Willkürlichkeit der Wahl von α_0 würde aus

$$\alpha_0 + \alpha_1 x_{\tau_1} + \alpha_2 x_{\tau_2} + \ldots = c_i (\alpha_0 + \alpha_1 x_{i_1} + \alpha_2 x_{i_2} + \ldots)$$

sofort

$$c_i = 1$$

sich ergeben, und daher die unmögliche Gleichung $\varphi_\tau = \varphi_{s_\alpha}$.

§ 31. In vielen Fällen ist die Berechnung von Φ unthunlich, da bei einigermassen grossem r die Multiplikationen nicht zu bewältigen sind. Man kann aber eine andere Bildungsart angeben, bei welcher das Produkt durch eine Summe ersetzt wird und jede Rechnungsschwierigkeit in Wegfall kommt.

Zuerst nehmen wir statt der linearen Funktion φ als Grundlage weiterer Bildungen folgende Funktion an

$$\psi(x_1, x_2, \ldots x_n) = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n};$$

die $\alpha_1, \alpha_2, \ldots \alpha_n$ sind hier wiederum willkürliche Konstanten, und aus ihrer und der x_λ Unabhängigkeit folgt, dass ψ eine $n!$-wertige Funktion ist. Denn wäre

$$\psi_\sigma = \psi_\tau,$$

also etwa identisch

$$x_1^{\beta_1} x_2^{\beta_2} \ldots x_n^{\beta_n} = x_1^{\gamma_1} x_2^{\gamma_2} \ldots x_n^{\gamma_n},$$

so müsste, wenn $\beta_1 \gtrless \gamma_1$ wäre, die Gleichung für beliebig viele, also für mehr als β_1, γ_1 Werte von x_1 bei unveränderten $x_2, x_3, \ldots x_n$ richtig sein. Daraus folgt $\beta_1 = \gamma_1$; dann hebt man und verfährt ebenso u. s. f.

Nun bilden wir, wenn die Resultate der Substitutionen von G auf ψ mit

$$\psi_{s_1} = \psi_1, \ \psi_{s_2}, \ \psi_{s_3}, \ \ldots \ \psi_{s_r}$$

bezeichnet werden, die Summe

$$\Psi = \psi_1 + \psi_{s_2} + \psi_{s_3} + \ldots + \psi_{s_r}$$

und führen den Beweis für die Zusammengehörigkeit von Ψ und G genau so, wie im vorigen Paragraphen bei Φ und G.

Anmerkung. Man kann hier durch eine gewisse Voraussetzung über die α den ψ einige neue Eigenschaften aufprägen. Es möge aus

$$\alpha_{i_1} + \alpha_{i_2} + \ldots + \alpha_{i_\lambda} = \alpha_{k_1} + \alpha_{k_2} + \ldots + \alpha_{k_\mu}$$

folgen, dass $\lambda = \mu$ ist und dass alle Summanden der linken Seite auch auf der rechten auftreten. Dieser Bedingung wird z. B. durch die Wahl

$$\alpha_2 > \alpha_1, \quad \alpha_3 > \alpha_1 + \alpha_2, \quad \alpha_4 > \alpha_1 + \alpha_2 + \alpha_3, \ldots$$

speziell durch die Annahmen

$$\alpha_1 = 0, \quad \alpha_2 = 1, \quad \alpha_3 = 2, \quad \alpha_4 = 4, \quad \alpha_5 = 8, \ldots$$

genügt. Die hieraus hervorgehenden Eigenschaften werden im dritten Kapitel § 55 besprochen und benutzt werden.

Beispiel. Wir wenden jetzt die beiden angegebenen Methoden auf die bereits oben betrachtete Gruppe mit $n = 4$, $r = 8$ an:

$$G = [1, (x_1 x_2), (x_3 x_4), (x_1 x_2)(x_3 x_4), (x_1 x_3)(x_2 x_4), (x_1 x_4)(x_2 x_3), (x_1 x_3 x_2 x_4), (x_1 x_4 x_3 x_2)].$$

Wir legen dabei zu Grunde (unter Benutzung des Symbols $i = \sqrt{-1}$)

$$\varphi = x_1 + i x_2 - x_3 - i x_4; \quad \psi = x_1^0 x_2 x_3^2 x_4^3;$$

dann ergeben sich folgende Rechnungen:

$$\begin{aligned}
\Phi = {} & (x_1 + i x_2 - x_3 - i x_4)(x_2 + i x_1 - x_3 - i x_4)(x_1 + i x_2 - x_4 - i x_3) \\
& (x_2 + i x_1 - x_4 - i x_3)(x_3 + i x_4 - x_1 - i x_2)(x_4 + i x_3 - x_2 - i x_1) \\
& (x_3 + i x_4 - x_2 - i x_1)(x_4 + i x_3 - x_1 - i x_2) \\
= {} & [(x_1 + i x_2 - x_3 - i x_4)(x_2 + i x_1 - x_3 - i x_4)(x_1 + i x_2 - x_4 - i x_3) \\
& (x_2 + i x_1 - x_4 - i x_3)]^2 \\
= {} & \{[(x_1 - x_3)^2 + (x_2 - x_4)^2][(x_1 - x_4)^2 + (x_2 - x_3)^2]\}^2.
\end{aligned}$$

$$\begin{aligned}
\Psi = {} & x_2 x_3^2 x_4^3 + x_1 x_3^2 x_4^3 + x_2 x_4^2 x_3^3 + x_1 x_4^2 x_3^3 + x_4 x_1^2 x_2^3 + x_3 x_2^2 x_1^3 \\
& + x_4 x_2^2 x_1^3 + x_3 x_1^2 x_2^3 \\
= {} & (x_1 + x_2) x_3^2 x_4^3 + (x_1 + x_2) x_4^2 x_3^3 + (x_3 + x_4) x_1^2 x_2^3 + (x_3 + x_4) x_2^2 x_1^3 \\
= {} & (x_1 + x_2)(x_3 + x_4) \cdot (x_1^2 x_2^2 + x_3^2 x_4^2).
\end{aligned}$$

Keine der beiden Methoden liefert unmittelbar einfache Resultate; aber von Φ können wir sofort zu

$$[(x_1 - x_3)^2 + (x_2 - x_4)^2][(x_1 - x_4)^2 + (x_2 - x_3)^2]$$

übergehen; von Ψ zu den beiden Funktionen

$$(x_1 + x_2)(x_3 + x_4) \quad \text{und} \quad x_1 x_2 + x_3 x_4,$$

von denen die letztere uns bereits bekannt ist. Aus der Form von Ψ ist ersichtlich, dass bei veränderten Exponenten andere und andere Funktionen zum Vorschein kommen. So gehören alle

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

zu G, und man erkennt aus den beiden Methoden allgemein, dass zu jeder Gruppe unendlich viele Funktionen gehören. Zu bemerken ist aber, dass man nicht alle Funktionen auf diese Art erhält. So gehört

$$x_1 x_2 + x_3 x_4 - (x_1 x_3 + x_2 x_4)$$

zur Gruppe

$$G = [1,\ (x_1x_2)(x_3x_4),\ (x_1x_3)(x_2x_4),\ (x_1x_4)(x_2x_3)],$$

ohne durch obige Methoden ableitbar zu sein.

§ 32. Wir nehmen jetzt die Elemente $x_1, x_2, \ldots x_n$ als nicht von einander unabhängig an.

Lehrsatz V. Auch wenn beliebige Beziehungen zwischen den x bestehen, wobei nur die Gleichheit zweier oder mehrerer Elemente ausgeschlossen ist, kann man $n!$-wertige lineare Funktionen derselben aufstellen.*

Wir gehen mit den Bezeichnungen der ersten Hälfte des vorigen Paragraphen von der dort aufgestellten linearen Funktion

$$\varphi = \alpha_0 + \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$$

und dem Produkte der Differenzen von $\varphi_1, \varphi_{s_2}, \varphi_{s_3}, \ldots \varphi_{s_r}$, nämlich von

$$\Pi(\varphi_\sigma - \varphi_\tau)$$

aus, wo das Produkt über alle $\frac{n!(n!-1)}{1.2}$ Kombinationen der Werte von φ erstreckt ist. Man erhält ausgeschrieben

$$\Pi(\varphi_\sigma - \varphi_\tau) = \Pi[\alpha_1(x_{\sigma_1} - x_{\tau_1}) + \alpha_2(x_{\sigma_2} - x_{\tau_2}) + \ldots + \alpha_n(x_{\sigma_n} - x_{\tau_n})]$$

und kann aus dem Produkte rechts diejenigen Faktoren aussondern, in denen der Koefficient von α_1 von selbst verschwindet; wir setzen

$$\Pi(\varphi_\sigma - \varphi_\tau) = \Pi(\varphi'_\mu - \varphi'_\nu)\,\Pi'[\alpha_1(x_{\sigma_1} - x_{\tau_1}) + \ldots + \alpha_n(x_{\sigma_n} - x_{\tau_n})].$$

Hier sind die φ' von α_1 unabhängig, und der Strich am zweiten Produktzeichen bedeutet, dass die Faktorenbildung sich nur über gewisse Kombinationen $\varphi_\sigma - \varphi_\tau$ zu erstrecken habe. Wäre nun die linke Seite für jede Wahl der α gleich Null, so müsste es auch die rechte Seite sein. Nimmt man aber $\alpha_2, \alpha_3, \ldots \alpha_n$ beliebig und α_1 so an, dass für alle Faktoren des zweiten Produkts

$$\alpha_1 \neq -\frac{\alpha_2(x_{\sigma_2} - x_{\tau_2}) + \ldots + \alpha_n(x_{\sigma_n} - x_{\tau_n})}{x_{\sigma_1} - x_{\tau_1}}$$

ist, so schliesst man nur eine endliche Anzahl von Werten, weniger als $n!$, für α_1 aus, und dann bleibt unter dieser Beschränkung das zweite Produkt sicher von Null verschieden. Folglich muss für jede Wahl von $\alpha_2, \alpha_3, \ldots \alpha_n$

$$\Pi(\varphi'_\mu - \varphi'_\nu) = \Pi''[\alpha_2(x_{\sigma_2} - x_{\tau_2}) + \alpha_3(x_{\sigma_3} - x_{\tau_3}) + \ldots + \alpha_n(x_{\sigma_n} - x_{\tau_n})]$$

Null sein. Man kann hier mit α_2 genau so verfahren, wie oben mit α_1, und kommt schliesslich zu einem Produkte, welches nur Faktoren $\alpha_n(x_{\sigma_n} - x_{\tau_n})$ enthält. Einer von diesen muss identisch Null sein; also wird in der zugehörigen Differenz $\varphi_\sigma - \varphi_\tau$ der Faktor jedes α_λ Null

* Vergl. G. Cantor: Clebsch Anm. V, 133.

werden; die Substitutionen σ und τ sind also entweder identisch oder sie setzen zwar Elemente um, aber dieselben sind einander gleich. Beides ist ausgeschlossen. Mit einer Verallgemeinerung dieses Satzes werden wir uns später zu beschäftigen haben.

---

§ 33. Durch die Lehrsätze III) und IV) ist eine Klassifikation der ganzen Funktionen von n Veränderlichen begründet. Jede Funktion gehört einer Gruppe von Substitutionen zu, jeder Gruppe entspricht eine unendliche Anzahl von Funktionen. Diese Zugehörigkeit ist nicht das einzige Band, welches die Funktionen verbindet, die sämtlich für dieselben Substitutionen ungeändert bleiben: wir werden auch eine entsprechende charakteristische, algebraische Beziehung finden, die nämlich, dass jede Funktion, welche zu einer Gruppe G gehört, sich durch jede andere zu derselben Gruppe gehörige rational ausdrücken lässt.

Es würde daher eine fundamentale Aufgabe der Algebra sein, alle für n Elemente existierenden Gruppen aufzustellen. In solcher Allgemeinheit bietet aber die Lösung unüberwundene Schwierigkeiten. Über die Existenz von Funktionen, welche eine gegebene Anzahl von Werten besitzen, wird in einem der nächsten Kapitel gesprochen werden; es wird sich zeigen, dass starke Einschränkungen in der Bildungsmöglichkeit von Gruppen zu konstatieren sind. So giebt es z. B. bei 7 Elementen keine Funktion, welche 3, 4, 5, 6 Werte besitzt; und wir werden den Satz ableiten, dass eine Funktion von n Elementen, welche mehr als zweiwertig ist, mindestens n Werte besitzen wird, wenn $n > 4$ ist, u. s. f.

Hier wollen wir uns nur mit der Konstruktion und den Eigenschaften der einfachsten und für unsere Zwecke wichtigsten Gruppen beschäftigen.*

§ 34. Bekannt ist uns vor allem die Gruppe der Ordnung $n!$; sie gehört den symmetrischen Funktionen zu; sie umfasst alle Substitutionen.

Wir haben im ersten Kapitel gesehen, dass jede Substitution aus Transpositionen zusammensetzbar ist. Enthält also eine Gruppe alle Transpositionen, so enthält sie alle überhaupt möglichen Substitutionen. Damit dies letztere stattfinde, reicht es aber auch schon aus, dass sie alle die Transpositionen in sich schliesse, welche ein bestimmtes Element, z. B. x_1 enthalten, also

$$(x_1 x_2),\ (x_1 x_3),\ (x_1 x_4),\ \ldots\ (x_1 x_n).$$

* Vgl. Serret: Cours d'algèbre supérieure II, § 416—429. Cauchy a. a. O.

Denn jede andere Transposition ist durch diese $n-1$ darstellbar, da ja eine jede $(x_\alpha x_\beta)$ aus drei anderen der obigen Reihe zusammensetzbar ist:

$$(x_\alpha x_\beta) = (x_1 x_\alpha)(x_1 x_\beta)(x_1 x_\alpha),$$

(wobei man wieder erkennt, dass die Faktorenfolge keine willkürliche ist). Nennen wir die betrachtete Gruppe die symmetrische, so können wir sagen:

Lehrsatz VI. Eine Gruppe von n Elementen $x_1, x_2, \ldots x_\alpha, \ldots x_n$, welche die $n-1$ Transpositionen

$$(x_\alpha x_1), (x_\alpha x_2), \ldots (x_\alpha x_{\alpha-1}), (x_\alpha x_{\alpha+1}), \ldots (x_\alpha x_n)$$

enthält, ist mit der symmetrischen Gruppe der n Elemente identisch.

Zusatz. Eine Gruppe, welche die Transpositionen

$$(x_\alpha x_\beta), (x_\alpha x_\gamma), \ldots (x_\alpha x_\vartheta)$$

enthält, umfasst alle Substitutionen der symmetrischen aus den Elementen $x_\alpha, x_\beta, x_\gamma, \ldots x_\vartheta$ gebildeten Gruppe.

§ 35. Wir kennen ferner eine Gruppe, welche aus allen Substitutionen besteht, die sich durch eine gerade Anzahl von Transpositionen zusammensetzen lassen. Denn alle diese und nur sie lassen jede zweiwertige Funktion ungeändert, und daher bildet ihr Komplex eine Gruppe. Sie mag die alternierende heissen. Wir suchen ihre noch unbekannte Ordnung r zu bestimmen. Es seien

I) $$s_1 = 1, s_2, s_3, \ldots s_r$$

alle Substitutionen der alternierenden Gruppe,

II) $$s'_1, s'_2, s'_3, \ldots s'_t$$

alle Substitutionen, die nicht zu I) gehören, die also aus einer ungeraden Anzahl von Transpositionen zusammengesetzt sind. Wir nehmen nun irgend eine Transposition σ, z. B. $\sigma = (x_1 x_2)$ und bilden die beiden Reihen

I') $$s_1\sigma, s_2\sigma, s_3\sigma, \ldots s_r\sigma$$

II') $$s'_1\sigma, s'_2\sigma, s'_3\sigma, \ldots s'_t\sigma,$$

dann ist jede Substitution von I') aus einer ungeraden, jede von II') aus einer geraden Anzahl von Transpositionen zusammengesetzt. Folglich gehört jede Substitution aus I') zu II), jede aus II') zu I). Ferner ist $s_\alpha\sigma \neq s_\beta\sigma$ und $s'_\alpha\sigma \neq s'_\beta\sigma$; denn aus der Gleichheit würde folgen

$$s_\alpha = s_\alpha(\sigma\,.\,\sigma) = (s_\alpha\sigma)\,\sigma = (s_\beta\sigma)\,\sigma = s_\beta(\sigma\,.\,\sigma) = s_\beta$$
$$s'_\alpha = s'_\alpha(\sigma\,.\,\sigma) = (s'_\alpha\sigma)\,\sigma = (s'_\beta\sigma)\,\sigma = s'_\beta(\sigma\,.\,\sigma) = s'_\beta,$$

da ja

$$\sigma\,.\,\sigma = (x_1 x_2)(x_1 x_2) = 1$$

ist. Es muss also $r \leqq t$ und $t \leqq r$ also $r = t$ sein. I) und II) enthalten ferner sämtliche möglichen Substitutionen: folglich ist $r + t = n!$ und

$$r = \tfrac{1}{2} n!.$$

Es möge hier bemerkt werden, dass es ausser der alternierenden keine zweite Gruppe Γ der Ordnung $\frac{1}{2} n!$ giebt. Die zu Γ gehörige Funktion φ_1 bliebe nämlich nur für $\frac{1}{2} n!$ Substitutionen ungeändert; sie besässe daher noch andere Werte. Wäre φ_2 ein zweiter ihrer Werte, σ eine Substitution, welche φ_1 in $\varphi_2 = \varphi_\sigma$ überführt und würde φ_1 für

III) $$\Gamma = [1, s'_2, s'_3, \ldots s'_{\frac{1}{2}n!}]$$

ungeändert bleiben, dann müsste φ_1 in φ_2 übergeführt werden durch alle Substitutionen

IV) $$\sigma, s'_2\sigma, s'_3\sigma, \ldots s_{\frac{1}{2}n!}\sigma;$$

denn s'_λ lässt φ_1 ungeändert und σ führt es in φ_2 über, also wird $s'_\lambda\sigma$ ebenfalls φ_1 in φ_2 verwandeln. Alle Substitutionen $s'_\alpha\sigma$ der Reihe IV) sind von einander verschieden; denn aus $s'_\alpha\sigma = s'_\beta\sigma$ würde $s_\alpha = s_\beta$ folgen; sie sind auch von den s'_γ verschieden, denn diese haben auf φ_1 eine andere Wirkung als jene. Folglich erschöpfen III) und IV) alle Substitutionen, und φ_1 ist zweiwertig; denn es ist keine Substitution vorhanden, welche φ_1 in einen dritten Wert überführen könnte. Die zugehörige Gruppe ist also die alternierende.

Lehrsatz VII. Es giebt bei n Elementen nur eine Gruppe der Ordnung $\frac{1}{2} n!$ Diese ist die alternierende; sie gehört zu den zweiwertigen Funktionen.

Wir können den hier ausgesprochenen Satz erweitern. Da der Beweis dem vorstehenden durchaus parallel läuft, so können wir ihn wohl übergehen. Der Satz lautet:

Lehrsatz VIII. Entweder gehören alle Substitutionen jeder beliebigen Gruppe zur alternierenden, oder genau die Hälfte von allen.

Zusatz. Diejenigen Substitutionen einer beliebigen Gruppe, welche zur alternierenden Gruppe gehören, bilden eine in jener enthaltene Gruppe, deren Ordnung entweder gleich der der ursprünglichen oder gleich der Hälfte derselben ist.

Die einfachsten, der alternierenden Gruppe angehörigen Substitutionen enthalten drei Elemente. Sie werden aus zwei Transpositionen gebildet $(x_\alpha x_\gamma)(x_\gamma x_\beta) = (x_\alpha x_\beta x_\gamma)$.

Wir bezeichnen $(x_1 x_2 x_3 \ldots x_m)$ als Cirkularsubstitutionen m^{ter} Ordnung. Dann folgt:

Lehrsatz IX. Enthält eine Gruppe von n Elementen die $n-2$ Cirkularsubstitutionen

$$(x_1 x_2 x_3),\ (x_1 x_2 x_4),\ \ldots\ (x_1 x_2 x_n),$$

so ist es die alternierende oder die symmetrische Gruppe.

Da man hat

$$(x_\alpha x_\beta x_\gamma) = (x_1 x_2 x_\alpha)(x_1 x_2 x_\gamma)(x_1 x_2 x_\beta)(x_1 x_2 x_\alpha)(x_1 x_2 x_\alpha)(x_1 x_2 x_\gamma)$$
$$(x_1 x_2 x_\alpha)(x_1 x_2 x_\gamma)(x_1 x_2 x_\gamma),$$

so folgt aus unserer Annahme, dass jede Cirkularsubstitution dritter Ordnung in der Gruppe vorkommt. Da ferner

$$(x_1 x_2 x_3)(x_1 x_4 x_3) = (x_1 x_2)(x_3 x_4),\quad (x_1 x_3 x_2)(x_1 x_4 x_2) = (x_1 x_3)(x_2 x_4),\ \ldots$$

ist, so folgt aus dem Zwischenresultate, dass alle Substitutionen vorhanden sind, die aus zwei, und folglich alle, die aus vier, sechs und jeder geraden Anzahl von Transpositionen gebildet sind. Damit ist der Satz bewiesen.

Es sei noch folgender Satz erwähnt, dessen Beweis keine Schwierigkeiten machen wird und also übergangen werden kann:

Lehrsatz X. Enthält eine Gruppe alle Cirkularsubstitutionen m^{ter} Ordnung, wobei m eine ungerade Zahl bedeutet, so enthält sie die alternierende Gruppe.

Endlich ist hier der Platz, ein Kennzeichen anzugeben, welches die Entscheidung darüber liefert, ob eine gegebene Substitution, in Cyklen ausgedrückt, der alternierenden Gruppe angehört oder nicht. Der Beweis wird auch hier nicht von nöten sein:

Lehrsatz XI. Enthält eine Substitution m Elemente in k Cyklen, so gehört sie zur alternierenden Gruppe oder nicht, je nachdem $m-k$ gerade oder ungerade ist.

§ 36. Schon eine einzige Substitution giebt Veranlassung zur Bildung einer Gruppe, indem man sie mit sich selbst multipliziert, oder ihre Potenzen bildet. Der Begriff der Potenz ist nach den Ausführungen von § 27 völlig bestimmt. Es ist

$$S^m = S^{m-1}.S = S.S^{m-1} = S^{m-2}S^2 = S^\alpha S^{m-\alpha} = S^\alpha.S^\beta.S^{m-\alpha-\beta} = \ldots$$

Die Ausführung des Potenzierens ergiebt sich gleichfalls aus dem Früheren. Will man von einem Cyklus, und in gleicher Weise von einer Substitution, die zweite, dritte, vierte, ... α^{te} Potenz nehmen, so schreibt man, um die neue Substitution zu bilden, hinter jedes vorhandene Element das zweit-, dritt-, viert-, ... α^{te} darauf folgende des betrachteten Cyklus. So erhält man aus $(x_1 x_2 x_3 x_4 x_5 \ldots)$ respektive $(x_1 x_3 x_5 \ldots)$ bei der zweiten, $(x_1 x_4 x_7 \ldots)$ bei der dritten, $(x_1 x_5 x_9 \ldots)$ bei der vierten

Potenz u. s. w. Dass bei diesem Vorgehen ein Cyklus in mehrere zerfallen kann, ist ersichtlich; es wird dies stets dann und nur dann geschehen, wenn die Anzahl der Elemente des Cyklus einen gemeinsamen Teiler > 1 mit dem Exponenten der Potenz besitzt; die Anzahl der zerfallenden Cyklen ist gleich dem Teiler. So wird

$$(x_1x_2x_3x_4x_5x_6)^2 = (x_1x_3x_5)(x_2x_4x_6)$$
$$(x_1x_2x_3x_4x_5x_6)^3 = (x_1x_4)(x_2x_5)(x_3x_6)$$
$$(x_1x_2x_3x_4x_5x_6)^4 = (x_1x_5x_3)(x_2x_6x_4)$$
$$(x_1x_2x_3x_4x_5x_6)^5 = (x_1x_6x_5x_4x_3x_2).$$

Ist m die Anzahl der Elemente des Cyklus, so wird seine m^{te}, $2m^{\text{te}}$, $3m^{\text{te}}$, ... Potenz, aber keine andere gleich 1;

$$(x_1x_2x_3x_4x_5x_6)^6 = (x_1x_2x_3x_4x_5x_6)^{12} = \ldots = 1.$$

Enthält eine Substitution mehrere Cyklen mit bez. m_1, m_2, m_3, ... Elementen, so ist die niedrigste Potenz derselben, welche gleich 1 wird, diejenige, deren Exponent r das kleinste gemeinsame Vielfache von m_1, m_2, m_3, ... ist;

$$[(x_1x_2x_3)(x_4x_5)(x_6x_7)]^6 = 1.$$

Dieser selbe Exponent r ist zugleich die Ordnungszahl für die aus der Substitution durch Potenzierung gebildete Gruppe. Denn berechnet man

$$s,\ s^2,\ s^3,\ \ldots\ s^{r-1},\ s^r = 1,$$

so wiederholen sich bei weiterer Fortsetzung die Glieder in derselben Reihenfolge

$$s^{r+1} = s,\ s^{r+2} = s^2,\ s^{r+3} = s^3,\ \ldots\ s^{2r-1} = s^{r-1},\ s^{2r} = s^r = 1$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

und die niedergeschriebenen Potenzen von s^1 bis s^r sind von einander verschieden, da aus

$$s^\lambda = s^{\lambda+\mu} = s^\lambda . s^\mu \quad (\lambda + \mu \leqq r)$$

folgen würde, was gegen die Voraussetzungen verstösst:

$$s^\mu = 1 \quad (\mu < r).$$

Jetzt ergiebt sich auch die Definition von Potenzen mit negativen Exponenten. Wir setzen

$$s^{-\varkappa} = s^{r-\varkappa} = s^{2r-\varkappa} = \ldots,$$

so dass man erhält

$$s^\varkappa s^{-\varkappa} = 1;$$

es hebt daher $s^\varkappa$ die Wirkung von $s^{-\varkappa}$ auf. Die negativen Potenzen werden wie die positiven gebildet, nur dass man je nach dem Exponenten -1, -2, -3, ... jedesmal ein, zwei, drei Glieder rückwärts

im Cyklus geht. Das letzte Glied des Cyklus gilt dabei als das dem ersten vorhergehende.

Es mag bemerkt werden, dass $(st)^{-1} = t^{-1}s^{-1}$ ist; denn es wird $(st)^{-1}.(st) = 1$, und daraus folgt durch rechtsseitige Multiplikation zuerst mit t^{-1}, dann mit s^{-1} die aufgestellte Gleichung.

Die einfachste zu dem Cyklus $s = (x_1 x_2 \ldots x_n)$ und seinen Potenzen gehörige Funktion ist

$$\varphi = x_1 x_2^2 + x_2 x_3^2 + \ldots + x_{m-1} x_m^2 + x_m x_1^2.$$

§ 37. Sind zwei Substitutionen s_α, s_β gegeben, und soll man die Gruppe niedrigster Ordnung finden, welche s_α, s_β enthält, so hat man nicht nur die Potenzen s_α^λ, s_β^μ zu bilden und unter einander zu multiplizieren, sondern man muss alle Komplexe

$$1;\quad s_\alpha^\lambda,\ s_\beta^\mu;\quad s_\alpha^\lambda s_\beta^\mu,\ s_\beta^\mu s_\alpha^\lambda;\quad s_\alpha^\lambda s_\beta^\mu s_\alpha^\nu,\ s_\beta^\mu s_\alpha^\lambda s_\beta^\varkappa;\ \ldots$$

aufstellen. Von den gefundenen Substitutionen behält man die von einander verschiedenen zurück und fährt hiermit so lange fort, bis alle bei einer Produktbildung von n Faktoren der Form s_α^λ, s_β^μ entstehenden Substitutionen schon unter den früheren enthalten sind. Dann sind nämlich die von $m+1$ Faktoren auf solche von höchstens m Faktoren reduzierbar und also auch schon unter den früheren enthalten. Die Gruppe ist demnach abgeschlossen.

Falls man $s_\beta s_\alpha = s_\alpha s_\beta^\mu$ hat, ist die Gruppe durch alle Substitutionen der Form $s_\alpha^\lambda s_\beta^\mu$ erschöpft. Denn es wird

$$\begin{aligned}
s_\beta^2 s_\alpha &= s_\beta . s_\alpha s_\beta^\mu = s_\alpha s_\beta^{2\mu},\\
s_\beta^3 s_\alpha &= s_\beta . s_\alpha s_\beta^{2\mu} = s_\alpha s_\beta^{3\mu}, \ \ldots\\
s_\beta^m s_\alpha &= s_\alpha s_\beta^{m\mu},\\
s_\beta^m s_\alpha^2 &= s_\alpha s_\beta^{m\mu} s_\alpha = s_\alpha^2 s_\beta^{m\mu^2},\\
s_\beta^m s_\alpha^3 &= s_\alpha^2 s_\beta^{m\mu^2} s_\alpha = s_\alpha^3 s_\beta^{m\mu^3}, \ \ldots\\
s_\beta^m s_\alpha^k &= s_\alpha^k s_\beta^{m\mu^k}.
\end{aligned}$$

Infolgedessen kann jedes Produkt aus drei Faktoren auf ein solches von nur zweien reduziert werden:

$$\begin{aligned}
s_\alpha^\varrho s_\beta^\sigma s_\alpha^\tau &= s_\alpha^{\varrho+\tau} s_\beta^{\mu^\tau . \sigma},\\
s_\beta^\varrho s_\alpha^\sigma s_\beta^\tau &= s_\alpha^\sigma s_\beta^{\tau+\varrho.\mu^\sigma}.
\end{aligned}$$

Damit ist der Lehrsatz bewiesen.

Es sei z. B.

$$s_1 = (x_1 x_2 x_3 x_4 x_5), \quad s_2 = (x_2 x_3 x_5 x_4),$$

so wird

$$s_2 s_1 = (x_1 x_2 x_4 x_3) = s_1^3 s_2.$$

Es giebt also in der Gruppe geringster Ordnung, welche s_1 und s_2 enthält, höchstens $5.4 = 20$ Substitutionen. Um zu erkennen, ob es weniger giebt, nehmen wir an, es wäre

$$s_1^{\alpha} s_2^{\beta} = s_1^{\gamma} s_2^{\delta},$$

dann würde hieraus folgen

$$s_1^{\alpha-\gamma} = s_2^{\delta-\beta}.$$

Es giebt aber in der Reihe der Potenzen von s_2 nur eine, welche einer Potenz von s_1 gleich ist; dies ist die nullte. Also wird $\alpha = \gamma$, $\delta = \beta$ sein müssen. Unsere Gruppe enthält wirklich 20 Substitutionen. Diese sind, wenn wir der Einfachheit halber nur die Indices aufschreiben:

$$\begin{array}{llll}
s_1^0 = 1, & s_2 = (2354), & s_2^2 = (25)(34), & s_2^3 = (2453), \\
s_1^1 = (12345), & s_1 s_2 = (1325), & s_1 s_2^2 = (15)(24), & s_1 s_2^2 = (1435), \\
s_1^2 = (13524), & s_1^2 s_2 = (1534), & s_1^2 s_2^2 = (14)(23), & s_1^2 s_2^3 = (1254), \\
s_1^3 = (14253), & s_1^3 s_2 = (1243), & s_1^3 s_2^2 = (13)(45), & s_1^3 s_2^5 = (1523), \\
s_1^4 = (15432), & s_1^4 s_2 = (1452), & s_1^4 s_2^2 = (12)(35), & s_1^4 s_2^3 = (1342).
\end{array}$$

Ganz ähnlich gestaltet es sich z. B. auch für

$$s_1 = (x_1 x_2 x_3 x_4 x_5 x_6 x_7), \quad s_2 = (x_2 x_4 x_3 x_7 x_5 x_6).$$

Im Falle, dass jedes $s_\beta^\mu s_\alpha$ $(\mu = 1, 2, 3 \ldots)$ auf die Form $s_\alpha^\varkappa s_\beta^\lambda$ gebracht werden kann, ist die Gruppe geringster Ordnung, welche s_α, s_β enthält, durch die Substitutionen der Form $s_\alpha^\varkappa s_\beta^\lambda$ erschöpft. Denn wir können ähnlich wie oben jede Substitution $s_\beta^\mu s_\alpha^\nu$ auf die Form bringen $s_\alpha^\varkappa s_\beta^\lambda$; dadurch ist der gewünschte Beweis dann auf den obigen zurückgeführt.

Wenn ferner s_β^q die Potenz mit niedrigstem Exponenten aus der Reihe s_β, s_β^2, ... ist, welche unter den Potenzen von s_α vorkommt, so enthält die Gruppe q mal so viele Substitutionen, als die Ordnung k von s_α beträgt. Denn zuerst kann man, wenn in $s_\alpha^\varkappa s_\beta^\lambda$ der Exponent λ grösser ist als $q-1$, s_β^λ durch ein $s_\alpha^\mu s_\beta^\nu$ ersetzen, wo $\nu \leq q-1$ ist. Es giebt also höchstens $q.k$ verschiedene Substitutionen $s_\alpha^\varkappa s_\beta^\lambda$. Wenn ferner

$$s_\alpha^\varkappa s_\beta^\lambda = s_\alpha^\mu s_\beta^\nu \quad (\lambda, \nu \leq q-1)$$

wäre, dann würde, wenn wir $\lambda > \nu$ annehmen,

$$s_\beta^{\lambda-\nu} = s_\alpha^{\mu-\varkappa} \quad (\lambda - \nu < q-1)$$

sein, also $\lambda = \nu$, $\mu = \varkappa$ sein müssen. Es giebt also wirklich $q.k$ verschiedene Substitutionen. Man sieht leicht ein, dass q ein Teiler der Ordnung r von s_β ist; denn man hat $s_\beta^r = 1 = s_\alpha^0$.

Sind drei Substitutionen s_α, s_β, s_γ so beschaffen, dass für jedes μ

$$s_\beta^\mu s_\alpha = s_\alpha^\delta s_\beta^\varepsilon, \quad s_\gamma^\mu s_\alpha = s_\alpha^\zeta s_\beta^\eta s_\gamma^\vartheta, \quad s_\gamma^\mu s_\beta = s_\alpha^\iota s_\beta^\varkappa s_\gamma^\lambda$$

wird, ist dann k die Ordnung von s_α, ferner s_β^q die niedrigste Potenz von s_β, welche $= s_\alpha^r$, endlich s_γ^t die niedrigste Potenz von s_γ, welche $= s_\alpha^\pi s_\beta^\varrho$ wird, so hat die Gruppe niedrigster Ordnung, welche s_α, s_β, s_γ enthält, die Ordnung kqt und ihre Substitutionen sind durch die Werte von

$$s_\alpha^\delta s_\beta^\varepsilon s_\gamma^\zeta \quad (\delta = 0, 1, \ldots k-1; \quad \mu = 0, 1, \ldots q-1; \quad \zeta = 0, 1, \ldots t-1)$$

ausgedrückt. Der Beweis hiervon ist einfach und schliesst sich dem obigen so genau an, dass wir ihn übergehen können.

§ 38. In die Kategorie dieser Sätze gehört auch der folgende: Sind

$$G = [1, s_2, s_3, \ldots s_r],$$
$$H = [1, t_2, t_3, \ldots t_{r'}]$$

zwei Gruppen von Substitutionen, zwischen denen die Beziehung besteht

$$s_\alpha t_\beta = t_\gamma s_\delta,$$

wie man α, β auch wählen möge, haben G, H überdies ausser der Einheit keine Substitution gemeinsam haben, so bilden alle

$$s_\alpha t_\beta \quad \text{oder alle} \quad t_\beta s_\alpha \quad (\alpha = 1, 2, \ldots r; \quad \beta = 1, 2, \ldots r')$$

eine Gruppe der Ordnung $r.r'$, welche G und H als „Untergruppen“ enthält.

Da

$$s_\alpha t_\beta \,.\, s_\gamma t_\delta = s_\alpha (t_\beta s_\gamma)\, t_\delta = s_\alpha s_\varepsilon \,.\, t_\zeta t_\delta = s_\mu t_\nu$$

ist, so bilden die $s_\alpha t_\beta$ eine Gruppe von höchstens $r.r'$ Substitutionen.

Wir zeigen ferner, dass alle diese von einander verschieden sind. Wäre etwa

$$s_\alpha t_\beta = s_\gamma t_\delta,$$

so folgte daraus

$$s_\gamma^{-1} s_\alpha = t_\delta t_\beta^{-1},$$

indem man beide Seiten der darüberstehenden Gleichung links mit s_γ^{-1} und rechts mit t_β^{-1} multipliziert. Nun ist $s_\gamma^{-1} s_\alpha$ eine Substitution von G; diese wäre gleich einer Substitution $t_\delta t_\beta^{-1}$ von H; also sind beide Produkte $= 1$:

$$s_\gamma^{-1} s_\alpha = 1, \quad t_\delta t_\beta^{-1} = 1,$$
$$s_\alpha = s_\gamma, \qquad t_\delta = t_\beta.$$

Daraus folgt, dass die Ordnung der neuen Gruppe $= r.r'$ ist. Wir bezeichnen sie durch das Symbol

$$K = \{G, H\}.$$

§ 39. Für die späteren Entwickelungen ist mehrfach eine Gruppe notwendig, deren Ordnung die Potenz einer Primzahl p wird. Ihre

Existenz und ihre Natur wird durch den Beweis des folgenden Satzes erkannt:

Lehrsatz XII. Bezeichnet p^f die höchste das Produkt $n! = 1.2.3 \ldots n$ teilende Potenz der Primzahl p, so giebt es eine Gruppe des Grades n und der Ordnung p^f.

Zuerst sei $n < p^2$, also $n = ap + b$ $(a, b < p)$; dann sind von den Zahlen $1, 2, 3, \ldots n$ nur die Zahlen $p, 2p, 3p, \ldots ap$ jede durch die erste Potenz von p teilbar, also ist $f = a$. Wir heben aus den n Elementen a Systeme von je p Elementen heraus und bilden aus jedem System einen Cyklus, nämlich

$$s_1 = (x_1^{\,1} x_2^{\,1} x_3^{\,1} \ldots x_p^{\,1}); \quad s_2 = (x_1^{\,2} x_2^{\,2} \ldots x_p^{\,2}); \quad \ldots \quad s_a = (x_1^{\,a} x_2^{\,a} \ldots x_p^{\,a})$$

(wobei die oberen Indices natürlich keine Potenzbezeichnungen sind), und die Gruppe, welche aus diesen gebildet ist, nämlich

$$G_1 = [s_1, s_1^{\,2}, \ldots s_2, s_2^{\,2}, \ldots s_a, s_a^{\,2}, \ldots] = \{s_1, s_2, \ldots s_a\}^*$$

wird die verlangte sein. Denn jedes s_λ bildet durch seine Potenzen eine Untergruppe der Ordnung p. Da keine dieser a Untergruppen mit der anderen ein Element gemeinsam hat, so ist nach Lehrsatz II)

$$s_\lambda^{\,\varrho} s_\mu^{\,\sigma} = s_\mu^{\,\sigma} s_\lambda^{\,\varrho},$$

und so kann jede mögliche zu G gehörige Kombination von Substitutionen $s_1^{\,\alpha}$, $s_2^{\,\beta}$, ... auf die Form

$$s_1^{\,\alpha} s_2^{\,\beta} s_3^{\,\gamma} \ldots s_a^{\,\nu} \quad (\alpha, \beta, \gamma, \ldots \nu = 0, 1, 2, \ldots p-1)$$

gebracht werden. G_1 hat also höchstens p^a Substitutionen. Es hat aber auch wirklich so viele, da alle jene p^a von einander verschieden sind. Denn aus

$$s_1^{\,\alpha} s_2^{\,\beta} s_3^{\,\gamma} \ldots s_a^{\,\nu} = s_1^{\,\alpha'} s_2^{\,\beta'} s_3^{\,\gamma'} \ldots s_a^{\,\nu'}$$

würde folgen

$$s_1^{\,-\alpha'} . s_1^{\,\alpha} = s_1^{\,\alpha - \alpha'} = s_2^{\,\beta'} s_3^{\,\gamma'} \ldots s_a^{\,\nu'} s_a^{\,-\nu} s_{a-1}^{\,-\mu} \ldots s_3^{\,-\gamma} s_2^{\,-\beta} = s_2^{\,\beta' - \beta} s_3^{\,\gamma' - \gamma} \ldots,$$

also, da s_1 mit s_2, s_3, ... keine Elemente gemein hat, $\alpha = \alpha'$ u. s. w.

Wird aber $n = p^2$, so erhält man $f = p + 1$, da die in der Folge $1, 2, 3, \ldots p^2$ die durch p teilbaren Zahlen $p, 2p, 3p, \ldots (p-1)p, pp$ sind. Wir bilden jetzt wie oben

---

* Die geschweifte Klammer soll sich bei der Gruppenbezeichnung dadurch von der eckigen unterscheiden, dass die angedeutete Gruppe die niedrigste ist, welche die in die geschweifte Klammer aufgenommenen Substitutionen enthält. Die geschweifte Klammer braucht also nicht alle r Substitutionen der Gruppe einzuschliessen, was bei der eckigen Klammer stets der Fall ist, sondern nur konstituierende Substitutionen. Letztere können auf vielerlei Arten gewählt werden. Vergl. auch die Bezeichnung am Schlusse des vorigen Paragraphen.

$$s_1,\ s_2,\ s_3,\ \dots\ s_p,$$

ferner aber noch die Substitution s_{p+1}, welche alle p^2 Elemente enthält

$$s_{p+1} = (x_1{}^1 x_1{}^2 x_1{}^3 \dots x_1{}^p x_2{}^1 x_2{}^2 \dots x_2{}^p x_3{}^1 \dots x_3{}^p \dots x_p{}^p).$$

Dann wird

$$G_2 = \{s_1, s_2, \dots s_p, s_{p+1}\}$$

die verlangte Gruppe sein. Denn zuerst sieht man, dass

$$\begin{aligned}
&s_1\ s_{p+1} = s_{p+1}\ s_2, \quad \dots\ s_\alpha\ s_{p+1} = s_{p+1}\ s_{\alpha+1}, \quad \dots\ s_p\ s_{p+1} = s_{p+1}\ s_1,\\
&s_1{}^\lambda s_{p+1} = s_{p+1}\ s_2{}^\lambda, \quad \dots\ s_\alpha{}^\lambda s_{p+1} = s_{p+1}\ s_{\alpha+1}{}^\lambda, \quad \dots\ s_p{}^\lambda s_{p+1} = s_{p+1}\ s_1{}^\lambda,\\
&s_1{}^\lambda s_{p+1}{}^2 = s_{p+1}{}^2 s_3{}^\lambda, \quad \dots\ s_\alpha{}^\lambda s_{p+1}{}^2 = s_{p+1}{}^2 s_{\alpha+2}{}^\lambda, \quad \dots\ s_p{}^\lambda s_{p+1}{}^2 = s_{p+1}{}^2 s_2{}^\lambda,\\
&s_1{}^\lambda s_{p+1}{}^\mu = s_{p+1}{}^\mu s_{\mu+1}{}^\lambda, \dots\ s_\alpha{}^\lambda s_{p+1}{}^\mu = s_{p+1}{}^\mu s_{\mu+\alpha}{}^\lambda, \quad \dots\ s_p{}^\lambda s_{p+1}{}^\mu = s_{p+1}{}^\mu s_p{}^\lambda
\end{aligned}$$

wird. Demnach kann man alle aus den $s_1,\ s_2, \dots s_{p+1}$ gebildeten Substitutionen ganz so, wie es bereits in § 37 geschah, auf die Form

$$s_1{}^\alpha s_2{}^\beta s_3{}^\gamma \dots s_p{}^\iota s_{p+1}{}^\varkappa \quad (\alpha, \beta, \gamma, \dots \varkappa = 0, 1, 2, \dots p-1)$$

bringen; hier muss aber gezeigt werden, dass s_{p+1} auch nur bis zur Potenz $\varkappa = p-1$ genommen zu werden braucht. Es ist

$$\begin{aligned}
&s_{p+1}{}^p = (x_1{}^1 x_2{}^1 x_3{}^1 \dots x_p{}^1)(x_1{}^2 x_2{}^2 \dots x_p{}^2) \dots (x_1{}^p x_2{}^p \dots x_p{}^p) = s_1 s_2 \dots s_p,\\
&s_{p+1}{}^{\alpha p} = s_1{}^\alpha s_2{}^\alpha \dots s_p{}^\alpha;
\end{aligned}$$

folglich kann, wenn $\varkappa > p$ wäre, die höchste in $s_{p+1}{}^\varkappa$ enthaltene Potenz von $s_{p+1}{}^p$ herausgenommen, nach der letzten Formel durch Potenzen von $s_1,\ s_2, \dots s_p$ ersetzt, und diese können an den gebührenden Stellen untergebracht werden.

Es fragt sich endlich nur noch, ob die entstehenden $p^{p+1} = p^f$ Substitutionen alle von einander verschieden sind. Wären zwei einander gleich

$$s_1{}^\alpha s_2{}^\beta \dots s_p{}^\delta s_{p+1}{}^\varepsilon = s_1{}^{\alpha'} s_2{}^{\beta'} \dots s_p{}^{\delta'} s_{p+1}{}^{\varepsilon'},$$

so würde folgen

$$s_{p+1}{}^{\varepsilon-\varepsilon'} = s_1{}^{\alpha'-\alpha} s_2{}^{\beta'-\beta} \dots s_p{}^{\delta'-\delta}.$$

Hier ruft die rechte Seite keine Änderung der oberen Indices bei den $x_\lambda{}^\mu$ hervor; die linke thut es, wenn nicht $\varepsilon = \varepsilon'$ ist; somit u. s. w.

Ist $n > p^2$, aber $n < p^3$, also $n = a p^2 + b p + c$ $(a, b, c < p)$, so wählt man aus den n Elementen $x_\lambda{}^\mu$ beliebige a Systeme von je p^2 Elementen und b beliebige andere von je p Elementen, bildet aus den ersteren a Gruppen G_2, aus den letzteren b Gruppen G_1. Die Vereinigung dieser $a+b$ Gruppen liefert die Gruppe G_3, welche den Forderungen entspricht. Denn das Produkt der Zahlen

$$(a-1)p^2+1,\ (a-1)p^2+2, \dots (a-1)p^2+p, \dots (a-1)p^2+p^2 \quad (a<p)$$

ist eben nur durch dieselbe Potenz von p teilbar, wie dasjenige von

$$1,\ 2, \dots p, \dots p^2.$$

Ist dagegen $n = p^3$, so kommt für

$$(p-1)p^2+1,\ (p-1)p^2+2,\ \ldots\ (p-1)p^2+p,\ (p-1)p^2+p^2=p^3$$

wegen des letzten Gliedes eine neue Einheit zum Exponenten hinzu, so dass in diesem Falle die Multiplikation der p Teilgruppen G_2 nicht genügt. Hier nimmt man dann, genau wie bei $n=p^2$, noch eine Substitution s hinzu, welche in einem einzigen Cyklus alle $p \cdot p^2$ Elemente vereinigt und deren p^{te} Potenz in die p Substitutionen zerfällt, welche dem s_{p+1} entsprechen; dann kann man ebenso wie in jenem Falle zeigen, dass die neue Gruppe G_3 allen Forderungen genügt. Zugleich wird ersichtlich, dass die angewendeten Schlüsse und Sätze allgemein giltig sind, und damit ist das aufgestellte Theorem bewiesen.

§ 40. Da alle Gruppen $G_1, G_2, G_3, \ldots$ in die Bildung jeder höheren Gruppe G eingehen, so erkennen wir:

Zusatz. Ist p^f die höchste Potenz der Primzahl p, welche $n!$ teilt, so kann man eine Reihe von Gruppen

$$1,\ G_1,\ G_2,\ G_3,\ \ldots\ G_\lambda,\ G_{\lambda+1},\ \ldots\ G_f$$

von n Elementen aufstellen, welche bez. die Ordnungen

$$1,\ p,\ p^2,\ p^3,\ \ldots\ p^\lambda,\ p^{\lambda+1},\ \ldots\ p^f$$

besitzen. Jede Gruppe G_λ $(\lambda < f)$ ist in der darauf folgenden $G_{\lambda+1}$ enthalten.

Drittes Kapitel.

Die verschiedenen Werte einer mehrwertigen Funktion und ihre algebraischen Beziehungen zu einander.

§ 41. Wir haben im vorigen Kapitel gezeigt, dass jeder Funktion der n Veränderlichen $x_1, x_2, \ldots x_n$ eine Substitutionengruppe zugehört, und dass umgekehrt jeder Gruppe unendlich viele Funktionen der Veränderlichen entsprechen. Die Untersuchung des Zusammenhanges, der zwischen verschiedenen zu derselben Gruppe gehörigen Funktionen besteht, wird später durchgeführt werden; zuerst liegt es uns ob, den Zusammenhang, der zwischen den einzelnen Werten einer mehrwertigen Funktion etwa vorhanden ist, und die algebraischen Beziehungen dieser Werte zu einander klarzulegen.

Wenn $\varphi(x_1, x_2, \ldots x_n)$ keine symmetrische Funktion ist, oder mit anderen Worten, wenn die Substitutionen $s_1 = 1, s_2, s_3, \ldots s_r$ der Gruppe G, die zu φ gehört, nicht alle möglichen $n!$ Substitutionen erschöpfen

$(r < n!)$, so nimmt φ unter der Wirkung irgend einer der übrigen Substitutionen σ_2 einen neuen Wert $\varphi_2 = \varphi_{\sigma_2}$ an.

Wir bilden jetzt eine Tabelle, deren erste Zeile aus den sämtlichen Substitutionen der Gruppe G bestehen möge:

$$s_1 = 1,\ s_2,\ s_3,\ \ldots\ s_r;\quad G;\quad \varphi_1.$$

Die zweite Zeile werde aus dieser durch rechtsseitige Multiplikation aller Substitutionen s_λ mit σ_2 erhalten. Es entsteht

$$\sigma_2,\ s_2\sigma_2,\ s_3\sigma_2,\ \ldots\ s_r\sigma_2;\quad G.\sigma_2;\quad \varphi_2.$$

Dann folgt [vergl. zweites Kapitel § 35] 1) dass alle Substitutionen dieser Zeile φ_1 in φ_2 überführen; denn es ist $\varphi_{s_\alpha\sigma_2} = \varphi_{\sigma_2}$, da $\varphi_{s_\alpha} = \varphi_1$ ist; 2) dass nur die Substitutionen dieser Zeile φ_1 in φ_2 umwandeln; denn ist τ eine Substitution, welche dies vollbringt, so wird

$$\varphi_{\tau\sigma_2^{-1}} = \varphi_{\sigma_2\sigma_2^{-1}} = \varphi_1$$

werden, also lässt $\tau\sigma_2^{-1}$ die Funktion φ_1 ungeändert; daher ist $\tau\sigma_2^{-1} = s_\lambda$ und $\tau = (\tau\sigma_2^{-1})\,\sigma_2 = s_\lambda\sigma_2$, was zu beweisen war; 3) dass alle Substitutionen dieser Zeile von einander verschieden sind; denn aus $s_\alpha\sigma_2 = s_\beta\sigma_2$ würde folgen $s_\alpha = s_\beta$; 4) dass alle Substitutionen dieser Zeile von denen der ersten verschieden sind; denn aus $s_\alpha\sigma_2 = s_\beta$ würde folgen $\sigma_2 = s_\alpha^{-1}s_\beta = s_\gamma$.

Erschöpfen die $2r$ Substitutionen s_α und $s_\alpha\sigma_2$ der beiden Zeilen noch nicht alle möglichen $n!$ Substitutionen $(r < \frac{1}{2}n!)$, so giebt es eine neue Substitution σ_3, welche dann auch einen neuen Wert von φ, $\varphi_{\sigma_3} = \varphi_3$ hervorruft, weil alle Substitutionen, die φ_1 oder φ_2 hervorrufen, bereits in den ersten beiden Zeilen stehen. Die hierdurch bedingte dritte Zeile unserer Tabelle

$$\sigma_3,\ s_2\sigma_3,\ s_3\sigma_3,\ \ldots\ s_r\sigma_3;\quad G.\sigma_3;\quad \varphi_3$$

hat wieder die soeben erwähnten vier Eigenschaften: sie enthält nur solche und auch alle diejenigen Substitutionen, welche φ in φ_3 umändern; sie enthält nur unter sich und gegen die der früheren Zeilen verschiedene Substitutionen. Sollten durch diese $3r$ Substitutionen noch nicht alle möglichen $n!$ erschöpft sein, so fährt man in gleicher Weise fort, bis alle $n!$ Substitutionen in den Zeilen von je r Substitutionen untergebracht sind.

Solchen Tabellenbildungen werden wir häufiger begegnen; es werden dabei stets die Eigenschaften auftreten: 1) alle Substitutionen einer Zeile besitzen eine besondere Eigentümlichkeit; 2) nur die Substitutionen dieser Zeile besitzen diese Eigentümlichkeit; 3) sie sind sämtlich von einander verschieden; und mitunter tritt auch die vierte Eigenschaft auf: 4) sie sind von denen der übrigen Zeilen verschieden.

Aus unseren Entwickelungen können wir nun die Schlüsse ziehen:

Lehrsatz I. Hat die mehrwertige Funktion $\varphi(x_1, x_2, \ldots x_n)$ im Ganzen ϱ Werte $\varphi_1, \varphi_2, \varphi_3, \ldots \varphi_\varrho$, und wird φ in diese einzelnen Werte durch die Anwendung gewisser Substitutionen z. B. $1, \sigma_2, \sigma_3, \ldots \sigma_\varrho$ übergeführt; ist ferner G, die Gruppe von $\varphi = \varphi_1$, von der Ordnung r, und enthält G die Substitutionen $s_1 = 1, s_2, s_3, \ldots s_r$, so kann man folgende Tabelle entwerfen:

$$\begin{array}{llllll}
\varphi_1; & s_1 = 1, & s_2, & s_3, & \ldots s_r; & G_1 \\
\varphi_2; & \sigma_2, & s_2\sigma_2, & s_3\sigma_2, & \ldots s_r\sigma_2; & G_1 . \sigma_2 \\
\varphi_3; & \sigma_3, & s_2\sigma_3, & s_3\sigma_3, & \ldots s_r\sigma_3; & G_1 . \sigma_3 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\varphi_\varrho; & \sigma_\varrho, & s_2\sigma_\varrho, & s_3\sigma_\varrho, & \ldots s_r\sigma_\varrho; & G_1 . \sigma_\varrho,
\end{array}$$

in der jede Substitutionenzeile alle diejenigen und nur die Substitutionen enthält, welche φ in den der Zeile vorangeschriebenen Wert von φ_1 umwandeln.

§ 42. Aus dem Umstande, dass alle Substitutionen dieser Tabelle von einander verschieden sind, und dass die ϱ Reihen der Tabelle alle Substitutionen erschöpfen, ergeben sich folgende Sätze:

Lehrsatz II. Die Ordnung r einer Gruppe G von n Elementen ist ein Teiler von $n!$

Lehrsatz III. Die Anzahl ϱ der Werte einer ganzen Funktion von n Elementen ist ein Teiler von $n!$

Lehrsatz IV. Das Produkt aus der Anzahl ϱ der Werte einer ganzen Funktion von n Elementen in die Ordnung r der zugehörigen Gruppe ist gleich $n!$

Durch den dritten Lehrsatz wird die Existenzmöglichkeit mehrwertiger Funktionen eingeschränkt; so wird es unter den Funktionen von fünf Elementen keine sieben- und keine achtwertigen geben; doch auch hierbei sind die Grenzen noch zu weit gezogen, wie die im fünften Kapitel durchzuführende Untersuchung beweisen wird.

§ 43. Die Ableitung der eben aufgestellten Sätze beruhte darauf, dass wir alle überhaupt möglichen Substitutionen durch Systeme von je r derselben $s_\lambda \sigma_\mu$ $(\lambda = 1, 2, \ldots r;\ \mu = 1, 2, \ldots \varrho)$ erschöpfen konnten.

Dieselben Schlüsse sind aber auch in dem allgemeineren Falle anwendbar, dass alle Substitutionen der zu φ gehörigen Gruppe G in der, zu einer anderen Funktion ψ gehörigen Gruppe H enthalten sind, dass also die Gruppe G ein Teil oder eine Untergruppe von H ist. Wir kommen von diesem allgemeinen Falle zu dem speziellen, im

§ 41 soeben behandelten zurück, indem wir die umfassendere Gruppe H als symmetrische Gruppe annehmen und von den dort gebrauchten Beweisen zu den hier notwendigen, indem wir lediglich statt der Worte „alle möglichen Substitutionen" die Worte „alle r_1 Substitutionen von H" einsetzen. Man erkennt dann, dass alle Substitutionen von H durch eine Anzahl von Zeilen mit je r Substitutionen der Form $s_\lambda \sigma_\mu$ $(\lambda = 1, 2, 3, \ldots r)$ erschöpft werden, und kommt zu den Sätzen:

Lehrsatz V. Sind alle r Substitutionen der Gruppe G unter denen der Gruppe H von der Ordnung r_1 enthalten, so ist r ein Teiler von r_1.

Lehrsatz VI. Sind zwei Funktionen φ und ψ derselben n Elemente gegeben, und behält ψ für alle Substitutionen, welche φ nicht ändern, gleichfalls seinen Wert bei, so ist die Anzahl ϱ der Werte von φ ein Vielfaches der Anzahl ϱ_1 der Werte von ψ. Der Fall $\varrho = \varrho_1$ ist dabei eingeschlossen.

Denn es ist

$$\varrho = \frac{n!}{r}, \quad \varrho_1 = \frac{n!}{r_1}; \quad \varrho : \varrho_1 = r_1 : r.$$

§ 44. Eine neue Erweiterung unserer Betrachtungen würde darin bestehen, dass die Gruppen G und H in einigen Substitutionen übereinstimmen. Dieser Fall kann sofort auf den des vorigen Paragraphen zurückgeführt werden. Wir benutzen dazu folgenden Satz:

Lehrsatz VII. Die gemeinsamen Substitutionen zweier Gruppen bilden eine neue Gruppe, deren Ordnung dann ein Teiler der Ordnung jeder der beiden Gruppen wird.

Denn gehören σ, τ sowohl G_1 als G_2 an, so wird auch $\sigma . \tau$ sowohl G_1 als G_2 angehören und sich also auch unter den gemeinsamen Substitutionen befinden. — Dasselbe lässt sich auch folgendermassen erkennen: Ist φ_1 eine zu G_1, φ_2 eine zu G_2 gehörige Funktion, so bleibt

$$\psi = \alpha\varphi_1 + \beta\varphi_2$$

bei beliebigen Konstanten α, β nur dann für eine Substitution ungeändert, wenn sowohl φ_1 als φ_2 es bleiben, also nur für die den Gruppen G_1 und G_2 gemeinsamen Substitutionen. Diese gehören zur Funktion ψ und bilden daher eine Gruppe H.

Zusatz. Die Ordnung jeder Gruppe H, welche aus allen oder einem Teile der zwei Gruppen G_1 und G_2 angehörigen Substitutionen besteht, ist einem Teiler von r_1 und r_2 gleich.

§ 45. Wir beschäftigen uns jetzt mit der Gruppe, welche zu einem anderen Werte, z. B. φ_2 der Funktion φ_1 gehört. Die Gruppe $G = G_1$ von φ_1 enthalte

$$s_1 = 1,\ s_2,\ s_3,\ \ldots\ s_r.$$

Es fragt sich, welche Substitutionen denjenigen Wert φ_2 ungeändert lassen, der durch die Substitution σ_2 aus φ_1 entsteht? Da φ_1 durch σ_2 in $\varphi_2 = \varphi_{\sigma_2}$ übergeführt wird, so wird umgekehrt φ_2 durch σ_2^{-1} in φ_1 verwandelt. Wendet man also nach einander die Substitutionen σ_2^{-1}, s_α, σ_2 an, so geht φ_2 durch die erste Operation in φ_1 über, die zweite lässt φ_1 ungeändert und die dritte verwandelt φ_1 rückwärts in φ_2. Es bleibt also φ_2 für jedes $\sigma_2^{-1} s_\alpha \sigma_2$ ungeändert. Wir konstruieren daher die Zeile

$$\sigma_2^{-1} s_1 \sigma_2 = 1,\quad \sigma_2^{-1} s_2 \sigma_2,\quad \sigma_2^{-1} s_3 \sigma_2,\ \ldots\ \sigma_2^{-1} s_r \sigma_2$$

und zeigen, dass diese auch alle Substitutionen der angegebenen Eigenschaft enthält. Es sei τ eine Substitution, welche φ_2 nicht ändert, dann wird $\tau\sigma_2^{-1}$ die Funktion φ_2 in φ_1 umwandeln; also ist

$$(\varphi_2)_{\tau\sigma_2^{-1}} = (\varphi_{\sigma_2})_{\tau\sigma_2^{-1}} = \varphi_{\sigma_2\tau\sigma_2^{-1}} = \varphi_1,$$

und daher $\sigma_2\tau\sigma_2^{-1}$ zur Gruppe G_1 gehörig; wir dürfen es gleich s_α setzen. Aus

$$\sigma_2\tau\sigma_2^{-1} = s_\alpha \quad \text{folgt} \quad \tau = \sigma_2^{-1}(\sigma_2\tau\sigma_2^{-1})\,\sigma_2 = \sigma_2^{-1} s_\alpha \sigma_2,$$

was zu beweisen war. Endlich erkennt man leicht, dass alle Substitutionen der obigen Zeile von einander verschieden sind; denn

$$\sigma_2^{-1} s_\alpha \sigma_2 = \sigma_2^{-1} s_\beta \sigma_2 \quad \text{ergiebt} \quad s_\alpha = s_\beta.$$

Aus diesen drei Eigenschaften folgt, dass die Substitutionen dieser Zeile diejenige Gruppe bilden, welche zu φ_2 gehört; sie heisse G_2. Die Gruppeneigenschaft lässt sich auch aus der formalen Bildung ableiten, da ja

$$(\sigma_2^{-1} s_\alpha \sigma_2)(\sigma_2^{-1} s_\beta \sigma_2) = \sigma_2^{-1} s_\alpha (\sigma_2\sigma_2^{-1}) s_\beta \sigma_2 = \sigma_2^{-1} s_\alpha s_\beta \sigma_2$$

ist; bilden nun, wie vorausgesetzt wurde, die s_α, s_β, ... eine Gruppe, so findet dasselbe mit den neuen Substitutionen statt.

Die durchgeführten Ableitungen gelten für alle anderen Werte φ_3, φ_4, ... φ_ϱ der Funktion φ; so gelangt man zum

Lehrsatz VIII. Sind φ_1, φ_2, ... φ_ϱ die ϱ Werte, welche die ganze ϱ-wertige Funktion φ annehmen kann, und gehören zu φ_1, φ_2, ... φ_ϱ die Gruppen G_1, G_2, ... G_ϱ; entstehen ferner φ_1, φ_2, ... φ_ϱ aus φ durch die Anwendung der Substitutionen $\sigma_1 = 1$, σ_2, ... σ_ϱ, so ist

$$G_1 = [s_1 = 1,\ s_2,\ s_3,\ \dots\ s_r]$$
$$G_2 = [\sigma_2^{-1} s_1 \sigma_2 = 1,\ \sigma_2^{-1} s_2 \sigma_2,\ \sigma_2^{-1} s_3 \sigma_2,\ \dots\ \sigma_2^{-1} s_r \sigma_2] = \sigma_2^{-1} G_1 \sigma_2$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$G_\varrho = [\sigma_\varrho^{-1} s_1 \sigma_\varrho = 1,\ \sigma_\varrho^{-1} s_2 \sigma_\varrho,\ \sigma_\varrho^{-1} s_3 \sigma_\varrho,\ \dots\ \sigma_\varrho^{-1} s_r \sigma_\varrho] = \sigma_\varrho^{-1} G_1 \sigma_\varrho.$$

§ 46. Die beiden Funktionen φ_1 und φ_2 unterscheiden sich von einander nur durch die Bezeichnung der in sie eingehenden Elemente x_λ; wir nennen zwei Funktionen, welche in diesem Falle sind, einander ähnlich oder von gleichem Typus. Deswegen müssen auch die beiden Gruppen G_1 und G_2 gleicherweise einander ähnlich oder von gleichem Typus sein. Ist dies a priori klar, so kann man doch auch durch die Art der Ableitung von $\sigma_2^{-1} s_\alpha \sigma_2$ aus s_α dieselbe Eigentümlichkeit beweisen, ja sogar, dass nicht nur die beiden Gruppen G_2 und G_1, sondern auch schon die beiden Substitutionen s_α und und $\sigma_2^{-1} s_\alpha \sigma_2$ einander ähnlich sind. Man nennt diese Art der Ableitung Transformation; $\sigma_2^{-1} s_\alpha \sigma_2$ ist die Transformierte von s_α durch σ_2, und so auch G_2 die transformierte Gruppe von G_1 durch σ_2; wir werden sie auch gelegentlich, wie oben geschah, durch

$$G_2 = \sigma_2^{-1} G_1 \sigma_2$$

bezeichnen. Wir beweisen jetzt die Ähnlichkeit von s und $\sigma^{-1} s \sigma$. Bilden etwa $x_1,\ x_2,\ \dots\ x_\alpha$ einen Cyklus von s und enthält σ die Elementfolgen $x_1 x_{i_1},\ x_2 x_{i_2} \dots x_\alpha x_{i_\alpha}$, dann ist nach unserer ersten Schreibweise

$$\sigma = \begin{pmatrix} x_1 & x_2 & \dots & x_\alpha & \dots \\ x_{i_1} & x_{i_2} & \dots & x_{i_\alpha} & \dots \end{pmatrix}.$$

Nun wird $\sigma^{-1} s \sigma$ das Element x_{i_1} durch x_1 und x_2 nach x_{i_2} führen und die Folge $x_1 x_2$ durch $x_{i_1} x_{i_2}$ ersetzen; ebenso $x_2 x_3$ durch $x_{i_2} x_{i_3}$ u. s. f., und endlich $x_\alpha x_1$ durch $x_{i_\alpha} x_{i_1}$. Der Cyklus $(x_1,\ x_2 \dots x_\alpha)$ in s ist also durch den Cyklus $(x_{i_1} x_{i_2} \dots x_{i_\alpha})$ in $\sigma^{-1} s \sigma$ ersetzt worden; so geht jeder Cyklus von s in einen andern von gleicher Elementenzahl über, und dieser entsteht aus jenem, wenn man s gewissermassen als Funktion auffasst und in dem Ausdrucke derselben die Substitution σ durchführt.

Wir sahen, dass die Funktion von vier Elementen

$$\varphi_1 = x_1 x_2 + x_3 x_4$$

drei Werte habe, und dass ihre Gruppe daher von der Ordnung $\frac{4!}{3} = 8$ sei.

Die Substitution $\sigma_2 = (x_2 x_3)$, welche nicht in G_1 enthalten ist, liefert den Wert

$$\varphi_2 = x_1x_3 + x_2x_4,$$

und $\sigma_3 = (x_2x_3)$ den dritten, von φ_1 und φ_2 verschiedenen Wert

$$\varphi_3 = x_1x_4 + x_2x_3.$$

Man erhält durch Transformation mit σ_2, σ_3 aus

$$G_1 = [1, (x_1x_2), (x_3x_4), (x_1x_2)(x_3x_4), (x_1x_3x_2x_4), (x_1x_3)(x_2x_4), (x_1x_4)(x_2x_3), (x_1x_4x_2x_3)]$$

die beiden zu φ_2 bez. φ_3 gehörigen Gruppen

$$G_2 = \sigma_2^{-1} G_1 \sigma_2 =$$
$$[1, (x_1x_3), (x_2x_4), (x_1x_3)(x_2x_4), (x_1x_2x_3x_4), (x_1x_2)(x_3x_4), (x_1x_4)(x_2x_3), (x_1x_4x_3x_2)],$$

$$G_3 = \sigma_3^{-1} G_1 \sigma_3 =$$
$$[1, (x_1x_4), (x_2x_3), (x_1x_4)(x_2x_3), (x_1x_3x_4x_2), (x_1x_3)(x_2x_4), (x_1x_2)(x_3x_4), (x_1x_2x_4x_3)].$$

§ 47. Zusatz I. Transformiert man eine Substitutionengruppe durch eine beliebige Substitution, so bilden die transformierten Substitutionen wiederum eine Gruppe.

Zusatz II. Die beiden im allgemeinen von einander verschiedenen Substitutionen $s_\alpha s_\beta$ und $s_\beta s_\alpha$ sind einander ähnlich. Denn es ist

$$s_\alpha s_\beta = s_\beta^{-1}(s_\beta s_\alpha) s_\beta.$$

Zusatz III. Es ist $s_\alpha s_\beta s_\alpha^{-1}$ die Transformierte von s_β durch s_α^{-1}.

Zusatz IV. Sind s_α, s_β zwei Substitutionen, von denen die erste die Ordnung r besitzt, und die zweite so beschaffen ist, dass ihre q^{te} Potenz, aber keine frühere unter den Potenzen von s_α erscheint; ist ferner die Transformierte von s_β durch s_α gleich einer Potenz von s_β, so hat die niedrigste aus s_α und s_β gebildete Gruppe die Ordnung $q.r$ (vergl. zweites Kapitel §§ 37 u. 38).

Zusatz V. Alle Substitutionen, durch deren Transformation eine gegebene Substitution s in eine ihrer Potenzen s^α verwandelt wird, bilden eine Gruppe.

Zusatz VI. Alle Substitutionen, durch deren Transformation eine gegebene Gruppe in sich selbst verwandelt wird, bilden eine Gruppe.

Zusatz VII. Sind zwei Substitutionen oder zwei Gruppen einander ähnlich, so giebt es Substitutionen, welche die eine

in die andere transformieren. Bei Substitutionen findet man die Transformierende sehr einfach; bei Gruppen geht man am besten auf zwei zugehörige, ähnliche Funktionen über und erkennt auch dann leicht, wie die Transformierenden zu bilden sind.

Zusatz VIII. Zwei Potenzen s^α, s^β derselben Substitution sind einander dann und nur dann ähnlich, wenn α, β denselben grössten gemeinsamen Teiler mit der Ordnung von s besitzen.

§ 48. Mit Hilfe des soeben eingeführten Begriffes der Transformation können wir zu folgendem Korollar der Sätze von § 43:

Zusatz IX. Enthält eine Gruppe eine Substitution der Primzahlordnung p, so ist ihre Ordnung r ein Vielfaches von p; enthält eine Gruppe G eine Untergruppe von der Ordnung p^α, wo p eine Primzahl bedeutet, so ist ihre Ordnung ein Vielfaches von p^α —

auch die Umkehrung beweisen, welche folgendermassen lautet:

Lehrsatz X. Ist die Ordnung r einer Gruppe G durch p^α, die Potenz einer Primzahl p teilbar, so enthält G Gruppen der Ordnung p^α.*

Es sei φ eine zur Gruppe G gehörige Funktion und ψ eine zu der im zweiten Kapitel § 39 nachgewiesenen Gruppe H gehörige Funktion, welche dieselben n Elemente wie G besitzt und als Ordnung die grösstmögliche in $n!$ enthaltene Potenz p^f der Primzahl p. Dann haben φ und ψ respektive $\frac{n!}{r}$ und $\varrho = \frac{n!}{p^f}$ Werte; diese seien

$$\varphi_1, \varphi_2, \varphi_3, \ldots \varphi_\lambda, \ldots \varphi_{\frac{n!}{r}} \quad \text{und} \quad \psi_1, \psi_2, \psi_3, \ldots \psi_\mu, \ldots \psi_\varrho$$

mit den zugehörigen Gruppen

$$G_1, G_2, G_3, \ldots G_\lambda, \ldots G_{\frac{n!}{r}} \quad \text{und} \quad H_1, H_2, H_3, \ldots H_\mu, \ldots H_\varrho.$$

Die G wie die H sind sämtlich die Transformierten eines beliebigen G_λ respektive H_μ; die G sind sämtlich von der Ordnung r, die H von der Ordnung p^f. Wir suchen unter den Gruppen $H_1, H_2, \ldots H_\varrho$ diejenige aus, welche möglichst viele Substitutionen mit G_1 gemeinsam hat. Es sei dies H_1. Ferner nennen wir K_1 die Gruppe, welche aus allen G_1 und H_1 gemeinsamen Substitutionen gebildet ist. Ihre Ordnung ist nach § 44 Zusatz ein Teiler von p^f; er heisse p^{f_1}. K_1 ist

* Cauchy a. a. O. p. 250 beweist diesen Satz für $\alpha = 1$. Herr L. Sylow gab die Verallgemeinerung Clebsch Ann. V, 584 — 594.

dann die Gruppe einer Funktion $a\varphi_1 + b\psi_1$, und unsere Annahme über H_1 führt zu der Einsicht, dass die Ordnung von K_1 nicht kleiner ist, als diejenige einer der Gruppen

$$K_2,\ K_3,\ \dots\ K_\nu,\ \dots\ K_\varrho,$$

welche zu den Funktionen

$$a\varphi_1 + b\psi_2,\ a\varphi_1 + b\psi_3,\ \dots\ a\varphi_1 + b\psi_\nu,\ \dots\ a\varphi_1 + b\psi_\varrho$$

gehören und respektive die Ordnungen

$$p^{\beta_2},\ p^{\beta_3},\ \dots\ p^{\beta_\nu},\ \dots\ p^{\beta_\varrho}\quad (\leqq p^{\beta_1})$$

besitzen mögen.

Wir betrachten jetzt sämtliche Werte von $a\varphi + b\psi$, nämlich

$$a\varphi_\lambda + b\psi_\mu \quad \left(\lambda = 1, 2, \dots \frac{n!}{r};\quad \mu = 1, 2, \dots \frac{n!}{p^f} = \varrho\right);$$

ihre Anzahl ist $\frac{n!}{r} \cdot \frac{n!}{p^f}$; wir gehen von $a\varphi_1 + b\psi_1$ aus und transformieren diesen Wert durch alle $n!$ Substitutionen. Die zu $a\varphi_1 + b\psi_1$ gehörige Gruppe K_1 hat die Ordnung p^{β_1}, also ist die Anzahl der verschiedenen Werte von $a\varphi_1 + b\psi_1$, welche durch Transformationen erlangt werden können, gleich $n!:p^{\beta_1}$.

Ist $\frac{n!}{p^{\beta_1}} < \frac{n!}{r} \cdot \frac{n!}{p^f}$, so sind durch diese erste Operation nicht alle Werte von $a\varphi_\lambda + b\psi_\mu$ erschöpft. Es sei $a\varphi_\sigma + b\psi_\tau$ einer von den noch nicht erhaltenen; dann gehört auch $a\varphi_{\sigma\cdot\sigma^{-1}} + b\psi_{\tau\sigma^{-1}} = a\varphi_1 + b\psi_{\tau\sigma^{-1}}$ zu diesen; denn könnte man von $a\varphi_1 + b\psi_1$ zu ihm durch irgend eine Transformation kommen, so würde die weitere Anwendung der Substitution σ auch zu $a\varphi_\sigma + b\psi_\tau$ führen. Wir gehen nun von

$$a\varphi_1 + b\psi_{\tau\sigma^{-1}} = a\varphi_1 + b\psi_m$$

mit der Gruppe K_m der Ordnung p^{β_m} aus; die Transformation durch alle $n!$ Substitutionen liefert dann $n!:p^{\beta_m}$ neue unter sich und von den früheren verschiedene Werte.

Ist auch noch $\frac{n!}{p^{\beta_2}} + \frac{n!}{p^{\beta_2}} < \frac{n!}{r} \cdot \frac{n!}{p^f}$, so gelten dieselben Schlüsse: Es giebt eine neue Funktion $a\varphi_\varkappa + b\psi_\lambda$, ebenso eine neue $a\varphi_1 + b\psi_n = a\varphi_{\varkappa\cdot\varkappa^{-1}} + b\psi_{\lambda\varkappa^{-1}}$ mit der Gruppe K_n von der Ordnung p^{β_n} und infolgedessen $n!:p^{\beta_n}$ neue durch Transformation aus $a\varphi_1 + b\psi_n$ ableitbare Werte.

In dieser Weise wird man sämtliche $\frac{n!}{r} \cdot \frac{n!}{p^f}$ Werte, welche $a\varphi_\lambda + b\psi_\mu$ annehmen kann, endlich erlangen. Daher ist zu setzen

$$\frac{n!}{r}\cdot\frac{n!}{p^f}=\frac{n!}{p^{\beta_1}}+\frac{n!}{p^{\beta_m}}+\frac{n!}{p^{\beta_n}}+\ldots,$$

und da β_1 grösser oder doch nicht kleiner als jedes der übrigen β ist, so wird der erste Summand der rechten Seite der kleinste sein oder doch zu den kleinsten gehören; die Summe rechts ist daher ein Vielfaches des ersten Summanden

$$\frac{n!}{r}\cdot\frac{n!}{p^f}=q\cdot\frac{n!}{p^{\beta_1}},\quad n!\,p^{\beta_1}=q\,.\,r\,.\,p^f.$$

Die höchste Potenz von p, welche die linke Seite der letzten Gleichung teilt, ist die $f+\beta_1^{\text{te}}$, folglich ist rechts r höchstens durch p^{β_1} teilbar. Da aber G von der Ordnung r die Gruppe K_1 von der Orddung p^{β_1} enthält, so ist r auch mindestens durch p^{β_1} teilbar; folglich können wir

$$r=p^{\beta_1}\,.\,t$$

setzen, wo t den Faktor p nicht mehr enthält.

Der Voraussetzung nach enthält r den Faktor p^α; es ist daher α gleich oder kleiner als β_1; im ersten Falle ist K_1 die durch den Lehrsatz geforderte Gruppe, im zweiten Falle ist es eine Untergruppe von K_1, deren Existenz im zweiten Kapitel § 40 nachgewiesen ist.

§ 49. Zu diesem Satze sind noch zwei Bemerkungen zu machen.

Die im Beweise des Lehrsatzes benutzte, im zweiten Kapitel § 39 abgeleitete Gruppe H war vollkommen unabhängig von der im vorigen Paragraphen gerade betrachteten Gruppe G; trotzdem fand sich in H eine Untergruppe K_1, welche mit der höchsten Untergruppe von G, die eine Primzahlpotenz p^{β_1} zur Ordnung hatte, ihrem Typus nach übereinstimmte. Denkt man sich also irgend eine nur mögliche Gruppe der Ordnung p^{β_1} und nimmt diese für G, so folgt, dass H eine Untergruppe desselben Typus besitzt. Daher ergiebt sich:

Zusatz I. Die im zweiten Kapitel § 39 konstruierte Gruppe der Ordnung p^f und des Grades n enthält in ihren Untergruppen alle Typen von Gruppen der Ordnungen p^α $(\alpha\leq f)$.

Ist $r=p^\alpha\,.\,p_1^{\alpha_1}\,.\,p_2^{\alpha_2}\ldots$, wo $p, p_1, p_2, \ldots$ die verschiedenen Primzahlen sind, welche r enthält, so giebt es in G Gruppen

$$\Gamma, \Gamma_1, \Gamma_2, \ldots$$

der Ordnung

$$p^\alpha, p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots$$

Bildet man eine Gruppe, welche alle diese $\Gamma, \Gamma_1, \Gamma_2, \ldots$ enthält,

$$G'=\{\Gamma, \Gamma_1, \Gamma_2, \ldots\},$$

so ist G' mindestens von der Ordnung r (Lehrsatz IX); G' ist ferner in G enthalten und daher gleich G. Also ist bewiesen:

Zusatz II. Eine Gruppe G der Ordnung $r = p^{\alpha} . p_1^{\alpha_1} . p_2^{\alpha_2} \ldots$ lässt sich aus je einer Untergruppe der Ordnung p^{α}, $p_1^{\alpha_1}$, $p_2^{\alpha_2}$, ... zusammensetzen.

Weitere Folgerungen aus dem Lehrsatze X) werden später abgeleitet (§ 121).

§ 50. Bei der im fünften Paragraphen aufgestellten Tabelle musste natürlich jene vierte Eigentümlichkeit solcher Tabellen, auf welche früher aufmerksam gemacht wurde, wegfallen: es konnten die Substitutionen der einzelnen Zeilen nicht sämtlich von einander verschieden sein. Denn jede Gruppe enthält ja die Substitution 1 und diese muss also ϱ mal vorkommen. In dem Beispiele von § 46 kommen ferner die drei Substitutionen

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

in jeder der drei Gruppen vor. Wir wollen allgemein untersuchen, wann es möglich ist, dass eine und dieselbe Substitution den zu sämtlichen einzelnen Werten $\varphi_1, \varphi_2, \varphi_3, \ldots \varphi_\varrho$ gehörigen Gruppen $G_1, G_2, \ldots G_\varrho$ angehört. Es wird sich zeigen, dass das obige Beispiel einen beachtenswerten Ausnahmefall bildet, indem im allgemeinen ausser der Substitution 1 keine andere besteht, welche alle Werte einer Funktion ungeändert lässt.*

Wendet man auf die Reihe $\varphi_1, \varphi_2, \varphi_3, \ldots \varphi_\varrho$ eine beliebige Substitution σ an, so erhält man

$$\varphi_\sigma, \ \varphi_{\sigma_2 \sigma}, \ \varphi_{\sigma_3 \sigma}, \ \ldots \ \varphi_{\sigma_\varrho \sigma};$$

diese Werte werden, abgesehen von der Reihenfolge, mit den ersteren übereinstimmen. Denn $\varphi_1, \varphi_2, \ldots \varphi_\varrho$ sind alle überhaupt möglichen Werte und die eben erlangten sind sämtlich von einander verschieden. Die zu der letzteren Reihe gehörigen Gruppen

$$\sigma^{-1} G_1 \sigma, \ \sigma^{-1} G_2 \sigma, \ \sigma^{-1} G_3 \sigma, \ \ldots \ \sigma^{-1} G_\varrho \sigma$$

sind daher, abgesehen von der Reihenfolge, auch mit $G_1, G_2, \ldots G_\varrho$ identisch, d. h. die Gesamtheit von $G_1, G_2, \ldots G_\varrho$ ändert sich bei der Transformation durch eine ganz willkürliche Substitution σ nicht. Bezeichnen wir nun mit H die Gruppe derjenigen Substitutionen, welche in $G_1, G_2, \ldots G_\varrho$ gemeinsam vorkommen, so ist H auch die Gruppe derjenigen Substitutionen, welche in $\sigma^{-1} G_1 \sigma, \ \sigma^{-1} G_2 \sigma, \ \ldots \ \sigma^{-1} G_\varrho \sigma$ ge-

* L. Kronecker: Monatsber. d. Berl. Akad. 1879, S. 208.

meinsam vorkommen. Diese letztere Gruppe ist natürlich auch durch $\sigma^{-1}H\sigma$ ausgedrückt; demgemäss ist

$$\sigma^{-1}H\sigma = H,$$

d. h. die Gruppe H ändert sich nicht, wenn man sie auf irgend eine Weise transformiert; sie enthält also alle Substitutionen, die einer in ihr enthaltenen ähnlich sind.

Wir untersuchen nun zunächst die Natur einer so beschaffenen Gruppe H. Wir betrachten diejenigen Substitutionen von H, welche, abgesehen von der identischen Substitution 1, möglichst wenige Elemente enthalten. Wir beweisen von diesen Substitutionen zuerst, dass in keinem ihrer Cyklen mehr als drei Elemente vorkommen können. Denn hätte man z. B.

$$s = (x_1 x_2 x_3 x_4 \ldots) \ldots,$$

so nehme man $\sigma = (x_3 x_4)$ und da $\sigma^{-1}H\sigma = H$ ist, so wird auch

$$\sigma^{-1}s\sigma = (x_1 x_2 x_4 x_3 \ldots) \ldots = s_1$$

in H vorkommen. s_1 unterscheidet sich dann von s nur in der Stellung der beiden Elemente x_3, x_4. Daher wird das Produkt beider Substitutionen, welches natürlich auch in H auftritt, da H eine Gruppe ist,

$$s \,.\, s_1 = (x_1 x_4 \ldots) \ldots (x_3)$$

sicher das Element x_3 nicht mehr enthalten, wohl aber die Folge $x_1 x_4$; ohne also $= 1$ zu sein, hat es weniger Elemente als s, was der Annahme widerspricht.

Zweitens beweisen wir, dass die Substitutionen von möglichst wenigen Elementen in H, falls der Grad $n > 4$ ist, nicht mehr als einen Cyklus enthalten können. Denn sonst käme in H eine der Substitutionen vor

$$s_\alpha = (x_1 x_2)(x_3 x_4)\ldots, \quad s_\beta = (x_1 x_4)(x_2 x_3 x_5)\ldots, \quad s_\gamma = (x_1 x_2 x_3)(x_4 x_5 x_6)\ldots$$

und dann auch die entsprechende durch $\sigma = (x_4 x_5)$ transformierte Substitution

$$s'_\alpha = (x_1 x_2)(x_3 x_5)\ldots, \quad s'_\beta = (x_1 x_5)(x_2 x_3 x_4)\ldots, \quad s'_\gamma = (x_1 x_2 x_3)(x_5 x_4 x_6)\ldots;$$

folglich enthielte H auch das entsprechende Produkt

$$s_\alpha^{-1} s'_\alpha = (x_3 \ldots)(x_1)(x_2)\ldots, \quad s_\beta^{-1} s'_\beta = (x_1 x_2)(x_4 x_5)(x_3)\ldots,$$
$$s_\gamma^{-1} s'_\gamma = (x_1)(x_2)(x_3)(x_4 x_5 x_6)\ldots$$

welches, ohne gleich 1 zu sein, weniger Elemente enthält, als das ursprünglich vorhandene s. Auch dies ist nicht möglich.

Ist also $n > 4$, so besteht H entweder aus der einzigen Substitution 1 oder es enthält H eine Substitution $(x_\mu x_\nu)$ oder eine Substitution $(x_\lambda x_\mu x_\nu)$.

Im zweiten Falle enthält H mit $(x_\mu x_\nu)$ alle Transformierten dieser Transposition; es ist somit H die symmetrische Gruppe. Im dritten Falle enthält H mit $(x_\lambda x_\mu x_\nu)$ alle Transformierten dieser Cirkularsubstitution dritter Ordnung; es ist also H die alternierende Gruppe (vergl. §§ 34, 35).

Von H gehen wir auf G zurück: Haben G_1, G_2, ... G_ϱ ausser der Einheit Substitutionen gemeinsam, so tritt der zweite oder der dritte Fall ein; H, welches in jedem G enthalten ist, umschliesst sicher die alternierende Gruppe, also ist auch G alternierend oder symmetrisch und $\varrho = 2$ oder $= 1$.

Ist dagegen $n = 4$, so könnte ausser $s_1 = 1$ noch ein

$$s_2 = (x_1 x_2)(x_3 x_4)$$

auftreten; hiermit zugleich müssten seine Transformierten, deren es nur zwei giebt,

$$s_3 = (x_1 x_3)(x_2 x_4) \quad \text{und} \quad s_4 = (x_1 x_4)(x_2 x_3),$$

vorhanden sein. Weitere Substitutionen könnte H nicht enthalten, ohne alternierend oder symmetrisch zu werden. Man hätte also die Ausnahmegruppe

$$H = [s_1 = 1,\ s_2,\ s_3,\ s_4];$$

diese geht in der That bei allen nur möglichen Transformationen in sich selbst über. Will man von ihr auf Gruppen G zurückgehen, so folgt aus § 43 Lehrsatz V), dass die Ordnung von G ein Vielfaches der Ordnung von H, also von 4 ist; aus Lehrsatz II) folgt, dass die Ordnung von G ein Teiler von $4! = 24$ ist, daher bleibt nur die Wahl zwischen den Zahlen 4, 8, 12, 24 als Ordnung von G. Die beiden letzten Zahlen führen auf die allgemeinen Fälle $\varrho = 2$, $\varrho = 1$. Der erste $r = 4$ liefert $H = G$, $\varrho = 6$ und z. B.

$$\varphi_1 = (x_1 x_2 + x_3 x_4) - (x_1 x_3 + x_2 x_4),\ \varphi_2 = (x_1 x_2 + x_3 x_4) - (x_1 x_4 + x_2 x_3),$$
$$\varphi_3 = (x_1 x_3 + x_2 x_4) - (x_1 x_4 + x_2 x_3),\ \varphi_4 = (x_1 x_3 + x_2 x_4) - (x_1 x_2 + x_3 x_4),$$
$$\varphi_5 = (x_1 x_4 + x_2 x_3) - (x_1 x_2 + x_3 x_4),\ \varphi_6 = (x_1 x_4 + x_2 x_3) - (x_1 x_3 + x_2 x_4).$$

Der zweite $r = 8$ liefert G als Vielfaches von H. Wir müssen also zu H noch Substitutionen hinzunehmen, um auf G zu kommen. Von der dritten Ordnung darf keine derselben sein, weil sonst $r = 12$ oder $= 24$ werden würde. Nimmt man irgend eine andere Substitution, so erhält man die in § 46 angeführte Gruppe, welche unter die im § 39 behandelten gehört. Für sie ist $\varrho = 3$ und z. B.

$$\psi_1 = x_1 x_2 + x_3 x_4, \quad \psi_2 = x_1 x_3 + x_2 x_4, \quad \psi_3 = x_1 x_4 + x_2 x_3.$$

Lehrsatz XI. Ist $n \gtrless 4$, so giebt es ausser den symmetrischen und den alternierenden Funktionen keine anderen,

deren sämtliche ϱ Werte für ein und dieselbe Substitution (ausser für die identischen Substitution) ungeändert bleiben. Für $n=4$ bleiben alle Funktionen, die zu den Gruppen von

$$\varphi=(x_1x_2+x_3x_4)-(x_1x_3+x_2x_4) \quad \text{oder von} \quad \psi=x_1x_2+x_3x_4$$

gehören, für die Substitutionen der Gruppe

$$H=[1,\ (x_1x_2)(x_3x_4),\ (x_1x_3)(x_2x_4),\ (x_1x_4)(x_2x_3)]$$

ungeändert.

---

§ 51. Wir haben bisher den substitutionen-theoretischen Zusammenhang der ϱ Werte einer ϱ-wertigen Funktion untersucht; jetzt gehen wir zur Betrachtung des algebraischen Zusammenhanges dieser Werte über.

Wir sahen am Anfange des vorigen Paragraphen, dass die Gesamtheit der Werte $\varphi_1, \varphi_2, \ldots \varphi_\varrho$ sich unter dem Einflusse einer beliebigen Substitution σ bis auf die Reihenfolge nicht ändert. Alle symmetrischen ganzen Funktionen von $\varphi_1, \varphi_2, \ldots \varphi_\varrho$ bleiben daher bei der Anwendung jeder beliebigen Substitution σ ungeändert und sind folglich nicht nur in den φ, sondern auch in den $x_1, x_2, \ldots x_n$ symmetrisch und daher durch die elementaren symmetrischen Funktionen c_λ der x_λ rational und ganz ausdrückbar. Bilden wir also

$$\begin{aligned}
S(\varphi_1) &= \varphi_1+\varphi_2+\ldots+\varphi_\varrho = R_1(c_1, c_2, \ldots c_n)\\
S(\varphi_1\varphi_2) &= \varphi_1\varphi_2+\varphi_1\varphi_3+\ldots = R_2(c_1, c_2, \ldots c_n)\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
S(\varphi_1\varphi_2\ldots\varphi_\varrho) &= \varphi_1\varphi_2\varphi_3\ldots\varphi_\varrho = R_\varrho(c_1, c_2, \ldots c_n),
\end{aligned}$$

so sind die R die Koefficienten einer Gleichung, deren Wurzeln φ_1, $\varphi_2, \ldots \varphi_\varrho$ werden.

Lehrsatz XII. Die ϱ Werte $\varphi_1, \varphi_2, \ldots \varphi_\varrho$ einer ϱ-wertigen rationalen ganzen Funktion φ sind die Wurzeln einer Gleichung ϱ^{ten} Grades

$$\varphi^\varrho - R_1\varphi^{\varrho-1}+R_2\varphi^{\varrho-2}-\ldots\pm R_\varrho=0,$$

deren Koefficienten rationale ganze Funktionen von den elementaren symmetrischen Funktionen $c_1, c_2, \ldots c_n$ der Elemente $x_1, x_2, \ldots x_n$ sind.

§ 52. Beispielshalber suchen wir die Gleichung auf, deren Wurzeln die drei Werte

$$\psi_1=x_1x_2+x_3x_4, \quad \psi_2=x_1x_3+x_2x_4, \quad \psi_3=x_1x_4+x_2x_3$$

sind, wobei x_1, x_2, x_3, x_4 die Wurzeln der Gleichung

$$f(x) \equiv x^4 - c_1 x^3 + c_2 x^2 - c_3 x + c_4 = 0$$

sein mögen. Zuerst findet man ganz unmittelbar

$$\varphi_1 + \varphi_2 + \varphi_3 = S(x_1 x_2) = c_2;$$

ferner wird nach Kapitel 1 § 10

$$\varphi_1 \varphi_2 + \varphi_1 \varphi_3 + \varphi_2 \varphi_3 = S(x_1^2 x_2 x_3) = \alpha c_4 + \beta c_1 c_3 + \gamma c_2^2.$$

Die Zahlenfaktoren α, β, γ ergeben sich durch numerische Beispiele gleich -4, 1, 0

$$\varphi_1 \varphi_2 + \varphi_1 \varphi_3 + \varphi_2 \varphi_3 = c_1 c_3 - 4 c_4.$$

Endlich ist

$$\begin{aligned} \varphi_1 \varphi_2 \varphi_3 &= S(x_1^2 x_2^2 x_3^2) + x_1 x_2 x_3 x_4 S(x_1^2) \\ &= c_1^2 c_4 - 4 c_2 c_4 + c_3^2. \end{aligned}$$

Folglich erhält man als Ausdrucksform der gesuchten Gleichung

$$g(\varphi) \equiv \varphi^3 - c_2 \varphi^2 + (c_1 c_3 - 4 c_4) \varphi - (c_1^2 c_4 - 4 c_2 c_4 + c_3^2) = 0.$$

Wir wollen die Diskriminante dieser Gleichung, respektive ihrer drei Wurzeln untersuchen. Hierbei gebrauchen wir nicht die fertigen früher aufgestellten Formeln, welche zu umständlichen Rechnungen führen würden, sondern wir bilden direkt

$$\begin{aligned} \varphi_1 - \varphi_2 &= (x_1 - x_4)(x_2 - x_3), \\ \varphi_2 - \varphi_3 &= (x_1 - x_2)(x_3 - x_4), \\ \varphi_3 - \varphi_1 &= (x_1 - x_3)(x_2 - x_4), \end{aligned}$$

und erhalten, wenn wir die Diskriminante der φ mit Δ_φ, diejenige der x mit Δ bezeichnen,

$$\begin{aligned} \Delta_\varphi &= (\varphi_1 - \varphi_2)^2 (\varphi_2 - \varphi_3)^2 (\varphi_3 - \varphi_1)^2 \\ &= (x_1 - x_2)^2 (x_1 - x_3)^2 (x_1 - x_4)^2 (x_2 - x_3)^2 (x_2 - x_4)^2 (x_3 - x_4)^2 = \Delta. \end{aligned}$$

Wir erkennen hierdurch nebenbei, dass die Diskriminante einer Gleichung vierten Grades $f(x) = 0$ auch als Diskriminante einer Gleichung dritten Grades gebildet werden kann. Wichtiger ist, dass der erlangte Spezialsatz sich nach einer anderen Seite hin erweitern lässt. Diese Erweiterung suchen wir auf.

§ 53. Wir legen unseren Betrachtungen die Tabelle aus § 41 zu Grunde. Ist φ nicht einwertig, so enthält die erste Zeile der Tabelle, d. h. die zu φ_1 gehörige Gruppe G nicht alle überhaupt möglichen Transpositionen. Kommt eine Transposition, z. B. $(x_\alpha x_\beta)$ in der zweiten Zeile der Tabelle vor, so ist dies gemäss der Konstruktion dieser Tabelle ein Zeichen dafür, dass φ_1 durch $(x_\alpha x_\beta)$ in φ_2 verwandelt wird. Es ist demnach für $x_\alpha = x_\beta$ auch $\varphi_1 = \varphi_2$, denn dann wird die Transposition $(x_\alpha x_\beta)$, welche aus φ_1 den Wert φ_2 hervorruft, auf φ_1 ja keine

Änderung ausüben. Es wird folglich $\varphi_1 - \varphi_2$ für $x_\alpha = x_\beta$ zu Null werden und also durch $x_\alpha - x_\beta$ teilbar sein.

Sobald daher eine Transposition $(x_\alpha x_\beta)$ in der Gruppe G von φ_1 nicht vorkommt, ist eine der Differenzen $\varphi_1 - \varphi_\lambda\,(\lambda = 2, 3, \ldots \varrho)$ durch einen Faktor von der Form $x_\alpha - x_\beta$ teilbar.

Nun giebt es bei n Elementen $\frac{n(n-1)}{2}$ Transpositionen. Enthält die erste Zeile unserer Tabelle, d. h. G_1, genau q von denselben, so bleiben in den übrigen Zeilen $\frac{n(n-1)}{2} - q$ zurück. Es wird daher das Produkt

$$(\varphi_1 - \varphi_2)(\varphi_1 - \varphi_3) \ldots (\varphi_1 - \varphi_\varrho)$$

durch $\frac{n(n-1)}{2} - q$ von einander verschiedene Differenzen der Form $(x_\alpha - x_\beta)$ teilbar sein und folglich auch durch das Produkt derselben.

Statt von φ_1 hätten wir auch von φ_2 ausgehen können. Da die zu $\varphi_2 = \varphi_{\sigma_2}$ gehörige Gruppe $G_2 = \sigma_2^{-1} G_1 \sigma_2$ der Gruppe G_1 ähnlich ist, so enthält auch sie q Transpositionen, und auch das Produkt

$$(\varphi_2 - \varphi_1)(\varphi_2 - \varphi_3) \ldots (\varphi_2 - \varphi_\varrho)$$

ist durch das Produkt von $\frac{n(n-1)}{2} - q$ Differenzen der Form $(x_\alpha - x_\beta)$ teilbar.

Dieselben Schlüsse gelten, wenn man $\varphi_3, \varphi_4, \ldots \varphi_\varrho$ zum Ausgangspunkt nimmt.

Multipliziert man die einzelnen Faktorenreihen, so wird

$$\Delta_\varphi = (-1)^{\frac{\varrho(\varrho-1)}{2}} \prod_{\lambda=1}^{\varrho} \{(\varphi_\lambda - \varphi_1)(\varphi_\lambda - \varphi_2) \ldots (\varphi_\lambda - \varphi_{\lambda-1})(\varphi_\lambda - \varphi_{\lambda+1}) \ldots \ldots (\varphi_\lambda - \varphi_\varrho)\}$$

durch das Produkt von $\varrho\left[\frac{n(n-1)}{2} - q\right]$ Differenzen $(x_\alpha - x_\beta)$ teilbar; Δ_φ ist in den x_λ symmetrisch; das Vorkommen von $(x_\alpha - x_\beta)$ als Faktor fordert demnach auch dasjenige jeder anderen Differenz $(x_\gamma - x_\delta)$ und damit auch das von $\Delta = \prod_{\alpha>\beta} (x_\alpha - x_\beta)^2$, der Diskriminante von $f(x)$. Es sei Δ^t die höchste Potenz von Δ, welche als Faktor in Δ_φ eingeht; dann muss Δ^t alle vorkommenden Differenzen $x_\alpha - x_\beta$ in sich schliessen, und da Δ deren $n(n-1)$ und somit Δ^t deren $n(n-1)t$ enthält, so muss

$$n(n-1)t \geq \varrho\left[\frac{n(n-1)}{2} - q\right]$$

$$t \geq \frac{\varrho}{2} - \frac{q\varrho}{n(n-1)}$$

sein. Diese Zahl t kann nur dann Null werden, wenn $q = \frac{n(n-1)}{2}$ ist, wenn also alle Transpositionen in G_1 vorkommen. Dann ist φ symmetrisch und $\varrho = 1$. q ist ferner dann und nur dann Null, wenn G keine Transpositionen enthält. Einer der Fälle, in denen dies eintritt, ist der, dass G die alternierende Gruppe oder eine Untergruppe derselben ist.

Lehrsatz XIII. Ist φ eine ϱ-wertige Funktion der n Elemente $x_1, x_2, \ldots x_n$, deren Gruppe q Transpositionen enthält, so hat die Diskriminante Δ_φ der ϱ Werte $\varphi_1, \varphi_2, \ldots \varphi_\varrho$ den Faktor

$$\Delta^{\varrho\left(\frac{1}{2} - \frac{q}{n(n-1)}\right)}.$$

Ist φ nicht symmetrisch, so ist der Exponent von Null verschieden. Ist die Gruppe von φ unter der alternierenden enthalten, so wird $q = 0$.

Alle mehrwertigen Funktionen enthalten demnach gleiche Werte, sobald zwei Elemente x einander gleich werden.

Hieraus erkennt man, warum es im zweiten Kapitel § 32 unmöglich war, bei gleichen Werten der x Funktionen von $n!$ Werten abzuleiten (vergl. auch § 104).

§ 54. Wir haben für t den unteren Wert $\frac{\varrho}{2} - \frac{q\varrho}{n(n-1)}$ gefunden. Dies heisst, dass die Diskriminante jeder beliebigen zur Gruppe G_1 gehörigen Funktion durch die angegebene Potenz von Δ teilbar ist. Es wäre aber wohl möglich, dass bei einigen oder gar bei allen Funktionen der Minimalwert von t überschritten würde.

Wir wollen annehmen, dass ein solches Überschreiten eintrete und dass der Exponent von Δ grösser als

$$\frac{\varrho}{2} - \frac{\varrho q}{n(n-1)}$$

wäre. Die hierbei auftauchenden Verhältnisse sollen jetzt zuerst untersucht werden. Eine höhere Potenz von $x_\alpha - x_\beta$ kann A) einmal dann eintreten, wenn $\varphi_1 - \varphi_\lambda$ durch $x_\alpha - x_\beta$ teilbar ist, ohne dass φ_1 durch $\sigma = (x_\alpha x_\beta)$ in φ_λ übergeführt würde; B) ferner dann, wenn φ_1 zwar durch $\sigma = (x_\alpha x_\beta)$ in φ_λ übergeführt wird, wenn aber $\varphi_1 - \varphi_\lambda$ durch eine höhere als die erste Potenz von $x_\alpha - x_\beta$ sich teilen lässt.

A) Im ersten Falle ist der Annahme nach

$$\varphi_1 - \varphi_\lambda = 0 \quad \text{für} \quad x_\alpha = x_\beta,$$

ohne dass $\varphi_\lambda = \varphi_\sigma$ wäre, wenn σ die Transposition $(x_\alpha x_\beta)$ bedeutet. Dann ist auch

$$\varphi_{\lambda\sigma} \neq \varphi_\sigma \quad \text{und} \quad \varphi_{\lambda\sigma} \neq \varphi_1,$$

da sonst wegen $\sigma^2 = 1$

$$\varphi_\lambda = \varphi_{\lambda\sigma^2} = \varphi_{\sigma^2} = \varphi_1, \quad \varphi_{\lambda\sigma^2} = \varphi_\lambda = \varphi_\sigma$$

wäre. Der allgemeine im vorigen Paragraphen besprochene Fall würde durch Kombination der vier von einander verschiedenen Werte φ_1, φ_λ, φ_σ, $\varphi_{\lambda\sigma}$ nur vier durch $x_\alpha - x_\beta$ teilbare Faktoren der Diskriminante

$$\varphi_\sigma - \varphi_1, \quad \varphi_1 - \varphi_\sigma; \quad \varphi_{\lambda\sigma} - \varphi_\lambda, \quad \varphi_\lambda - \varphi_{\lambda\sigma}$$

liefern. Unter unserer jetzigen Annahme, dass $\varphi_1 - \varphi_\lambda$ durch $x_\alpha - x_\beta$ teilbar sei, ohne dass $\varphi_\lambda = \varphi_\sigma$ ist, erhalten wir noch acht durch $x_\alpha - x_\beta$ teilbare Differenzen, die im obigen Falle nicht aufgetreten wären:

$$\varphi_\lambda - \varphi_1, \quad \varphi_1 - \varphi_\lambda; \quad \varphi_{\lambda\sigma} - \varphi_\sigma, \quad \varphi_\sigma - \varphi_{\lambda\sigma},$$
$$\varphi_\lambda - \varphi_\sigma, \quad \varphi_\sigma - \varphi_\lambda; \quad \varphi_{\lambda\sigma} - \varphi_1, \quad \varphi_1 - \varphi_{\lambda\sigma}.$$

Die Teilbarkeit der beiden ersten ist durch die Voraussetzungen gegeben; die der beiden nächsten ergiebt sich durch die Anwendung von σ auf die beiden ersten, denn hierdurch wird die Differenz $x_\alpha - x_\beta$ nur in $x_\beta - x_\alpha$ umgeändert, die Teilbarkeit also nicht aufgehoben. Die Teilbarkeit der letzten vier Differenzen folgt aus den Gleichungen

$$\varphi_\lambda - \varphi_\sigma = (\varphi_\lambda - \varphi_1) - (\varphi_\sigma - \varphi_1); \quad \varphi_{\lambda\sigma} - \varphi_1 = (\varphi_{\lambda\sigma} - \varphi_\sigma) - (\varphi_1 - \varphi_\sigma).$$

Tritt also der Faktor $x_\alpha - x_\beta$ überhaupt einmal überzählig auf, indem $\varphi_1 - \varphi_\lambda$ durch $x_\alpha - x_\beta$ teilbar, aber $\varphi \neq \varphi_\sigma$ ist, so tritt dieser Faktor acht mal überzählig auf. Wegen der symmetrischen Bildung von Δ_φ tritt also jeder Faktor dann acht mal überzählig auf, und da Δ ein Quadrat wird, tritt Δ vier mal überzählig als Faktor von Δ_φ auf.

B) Im zweiten Falle, in welchem $\varphi_1 - \varphi_\sigma$ oder $\varphi_1 - \varphi_\lambda$ durch eine höhere als die erste Potenz von $x_\alpha - x_\beta$ teilbar ist, lässt sich zeigen, dass die höchste Potenz dieser Differenz, welche als Teiler auftritt, bei $\varphi_1 - \varphi_\sigma$ eine ungerade Potenz von $(x_\alpha - x_\beta)$ zum Teiler hat, bei $\varphi_1 - \varphi_\lambda$ dagegen vier mal überzählig erscheint; auch hier wird die überzählig hinzutretende Potenz von Δ also eine gerade sein.

Es sei $(x_\alpha - x_\beta)^\nu$ die höchste Potenz von $x_\alpha - x_\beta$, welche $\varphi_1 - \varphi_\sigma$ teilt, so dass

$$\varphi_1 - \varphi_\sigma = (x_\alpha - x_\beta)^\nu \chi(x_1, x_2, \ldots x_\alpha, \ldots x_\beta, \ldots x_n)$$

befriedigt wird, ohne dass χ noch durch $x_\alpha - x_\beta$ teilbar wäre. Wendet man σ an, so folgt

$$\varphi_\sigma - \varphi_1 = (-1)^\nu (x_\alpha - x_\beta)^\nu \chi(x_1, x_2, \ldots x_\beta, \ldots x_\alpha, \ldots x_n)$$

und durch Addition der beiden letzten Gleichungen

$$0 = (x_\alpha - x_\beta)^\nu [\chi(\ldots x_\alpha, \ldots x_\beta, \ldots) + (-1)^\nu \chi(\ldots x_\beta, \ldots x_\alpha, \ldots)].$$

Da $(x_\alpha - x_\beta)^\nu \neq 0$ ist, muss der zweite Faktor $= 0$ sein; wäre ν gerade, so würde aus

$$\chi(\ldots x_\alpha, \ldots x_\beta, \ldots) = -\chi(\ldots x_\beta, \ldots x_\alpha, \ldots)$$

bei Gleichsetzung von x_α und x_β sich ergeben, dass $\chi(\ldots x_\alpha, \ldots x_\alpha, \ldots) = 0$ und dass folglich $\chi(\ldots x_\alpha, \ldots x_\beta, \ldots)$ gegen die über ν gemachte Voraussetzung noch durch einen Faktor $x_\alpha - x_\beta$ teilbar wäre. ν ist also ungerade.

Wäre endlich $\varphi_1 - \varphi_\lambda$, wo $\varphi_\lambda \neq \varphi_\sigma$ ist, durch eine höhere als die erste Potenz von $x_\alpha - x_\beta$ teilbar, so würde dieselbe Potenz vier mal, nämlich in

$$\varphi_1 - \varphi_\lambda, \quad \varphi_\lambda - \varphi_1; \quad \varphi_\sigma - \varphi_{\lambda\sigma}, \quad \varphi_{\lambda\sigma} - \varphi_\sigma$$

heraustreten. Also auch hier wäre der überzählige Exponent von Δ ein Vielfaches von 2.

Lehrsatz XIV. Ist φ_1 eine zur Gruppe G_1 gehörige Funktion und bedeutet g' den höchsten Exponenten, für welchen Δ_φ durch $\Delta^{g'}$ teilbar ist, so wird dieser Exponent den Wert

$$g' = \tfrac{1}{2}\varrho - \frac{\varrho q}{n(n-1)} + 2m, \quad m \geq 0$$

erhalten; ϱ bedeutet die Wertzahl von φ_1; n die Zahl der Elemente; q diejenige der in G_1 enthaltenen Transpositionen; m ist nur von der Natur von φ_1, nicht von der Gattung, der φ angehört, abhängig.

Beispiel zu A:

$$\begin{aligned} \psi_1 &= (x_1 - x_2)(x_3 - x_4) + S(x_1 x_2), \\ \sigma &= (x_1 x_2), \quad \lambda = (x_4 x_5), \\ \psi_\lambda &= (x_1 - x_2)(x_3 - x_5) + S(x_1 x_2), \\ \psi_1 - \psi_\lambda &= (x_1 - x_2)(x_5 - x_4). \end{aligned}$$

Es ist also $\psi_1 - \psi_\lambda$ durch $x_1 - x_2$ teilbar, trotzdem ψ_σ von ψ_λ verschieden ist.

Beispiel zu B:

$$\Delta_{\sqrt{\Delta}} = [(+\sqrt{\Delta}) - (-\sqrt{\Delta})]^2 = 4\Delta,$$

aber

$$\Delta_{\sqrt{\Delta^3 + \Sigma x}} = [(+\sqrt{\Delta^3 + \Sigma x}) - (-\sqrt{\Delta^3 + \Sigma x})]^2 = 4\Delta^3.$$

§ 55. Um zu zeigen, dass die eben behandelten Fälle nicht die allgemeinen sind, bilden wir eine Funktion der Gattung G gemäss der Anmerkung von § 31. Es sei

$$\psi_1 = \sum_r x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \dots x_{i_n}^{\alpha_n},$$

wo die Exponenten α so gewählt sind, dass aus der Gleichheit

$$\alpha_a + \alpha_b + \alpha_c + \dots = \alpha_d + \alpha_e + \dots$$

die Gleichheit der Indices $a, b, c, \dots$ mit denen der rechten Seite $d, e, \dots$ folgt. Es möge

$$\psi_1 - \psi_2 = 0$$

werden für die Annahmen

$$\alpha) \qquad x_{a'} = x_{a''} = \dots = x_{a^\nu}, \quad x_{b'} = x_{b''} = \dots = x_{b^\pi}, \dots$$

Da $x_{a'}, x_{b'}, \dots$ noch immer von einander unabhängig sind, und da $\psi_1 - \psi_2$ gleichviele positive und negative Summanden, jeden mit dem Koefficienten 1 behaftet, enthält, so kann die Differenz

$$\psi_1 - \psi_2 = \sum (x_{a'}^{\alpha_1 + \dots} x_{b'}^{\alpha_2 + \dots} \dots - x_{a'}^{\alpha_\varkappa + \dots} x_{b'}^{\alpha_\lambda + \dots} \dots)$$

nur verschwinden, wenn je ein Glied von dem durch α) modifizierten ψ_1 gegen ein Glied des gleichfalls modifizierten ψ_2 sich weghebt. Kommt dies z. B. bei

$$\beta) \qquad x_{a'}^{\alpha_1 + \dots} x_{b'}^{\alpha_2 + \dots} \dots \quad \text{und} \quad \beta') \quad x_{a'}^{\alpha_\varkappa + \dots} x_{b'}^{\alpha_\lambda + \dots} \dots$$

vor, so folgt die Gleichheit der Exponenten gleicher x in β) und β'), und daraus folgt nach der Annahme über die α, dass in zwei nicht modifizierten, sich nachher zerstörenden Gliedern von ψ_1 und ψ_2 die zu den $x_{a'}, x_{a''}, \dots$ gehörigen Komplexe von Exponenten einander gleich sind, ebenso die zu den $x_{b'}, x_{b''}, \dots$ gehörigen Komplexe von Exponenten u. s. w. Man kann daher eine oder mehrere Substitutionen σ konstruieren, welche β) dadurch in β') überführen, dass sie nur die $x_{a'}, x_{a''}, \dots$ unter sich, die $x_{b'}, x_{b''}, \dots$ unter sich u. s. w. umsetzen. Da hierdurch ein Term von ψ_1 in einen von ψ_2 übergeführt wird, und da alle $n!$ Terme der Form $x_1^{\alpha_1} x_2^{\alpha_2} \dots$ von einander verschieden sind und sich auf die ϱ Werte von ψ_1 verteilen, so führt σ ψ_1 völlig in ψ_2 über. Wird also in unserem Falle $\psi_1 - \psi_2 = 0$ für $x_{a'} = x_{a''}$, so wird $\sigma = (x_{a'} x_{a''})$ und $\psi_2 = \psi_\sigma$: der Fall A) § 54 ist daher ein Spezialfall.

Ist ferner, um nachzuweisen, dass auch B) § 54 den Charakter der Allgemeinheit entbehrt,

$$\gamma) \quad \psi_1 - \psi_\sigma = (x_{a'} - x_{a''}) \sum_r \frac{x_{a'}^{\alpha_1} x_{a''}^{\alpha_2} - x_{a''}^{\alpha_1} x_{a'}^{\alpha_2}}{x_{a'} - x_{a''}} x_b^\beta x_c^\gamma x_d^\delta \dots,$$

so werden in den r Summanden die Ausdrücke $x_b^{\beta} x_c^{\gamma} x_d^{\delta} \ldots$ sämtlich von einander verschieden sein. Denn es könnten zwei nur dann einander gleich sein, wenn in ψ_1 zwei Terme existierten, die sich nur durch die Exponenten zweier Potenzen $x_{a'}^{\alpha_1}$, $x_{a''}^{\alpha_2}$ von einander unterschieden, also durch die Substitution $\sigma = (x_{a'} x_{a''})$ in einander übergingen. Dann gehörte aber σ der Gruppe G_1 an, was der Voraussetzung widerspräche. Sollte demnach die rechte Seite von $\gamma)$ eine höhere als die erste Potenz von $(x_{a'} - x_{a''})$ enthalten, so müsste jeder einzelne Summand der Summe $(x_{a'} - x_{a''})$ enthalten; dies ist aber unmöglich, da jeder einzelne Summand nach der Durchführung der Division in eine Reihe von Gliedern mit gleichen Vorzeichen zerlegt wird. B) bildet also auch einen Spezialfall.

§ 56. Wir kennen demnach die höchste Potenz

$$\Delta^g, \quad g = \frac{\varrho}{2} - \frac{\varrho q}{n(n-1)},$$

der Diskriminante von $f(x)$, welche in allen Diskriminanten von Funktionen φ der Gattung G als Faktor enthalten ist. Gesetzt, alle diese enthielten noch einen gemeinsamen Faktor, der zuerst als Funktion der c_λ auftritt, dann aber in eine Funktion der x_λ umgewandelt und in Faktoren zerlegt gedacht werden kann; dann wird jeder dieser irreduktiblen Faktoren mehr als zwei Wurzeln x_λ oder, wenn nur zwei, dieselben in der Verbindung $x_\alpha + m x_\beta$ $(m \neq -1)$ umfassen; denn $x_\alpha - x_\beta$ riefe eine Potenz von Δ hervor. Dann könnte dieser Faktor und damit die Diskriminante jeder Funktion der Gattung zum Verschwinden gebracht werden, indem man zwischen den x_λ Beziehungen festsetzte, welche nicht in der Gleichsetzung zweier x_λ bestehen. Kann man also beweisen, dass trotz beliebiger Beziehungen zwischen den x_λ, die nur nicht in der Gleichsetzung zweier x_λ bestehen, dennoch jede Gattung Funktionen mit nicht verschwindender Diskriminante enthält, so ist die Annahme eines neuen, nicht gemeinsamen Faktors ausser Δ^g beseitigt. Der eben angeführte Satz wird in einem späteren Kapitel bewiesen. Antizipieren wir ihn, so folgt als Abschluss der letzten Untersuchungen:

Lehrsatz XV. *Δ^g ist der grösste gemeinsame Teiler aller Diskriminanten der zur Gattung G gehörigen Funktionen.*

§ 57. Wir kehren nunmehr zu der Gleichung zurück, deren Wurzeln $\varphi_1, \varphi_2, \ldots \varphi_\varrho$ sind

$$\varphi^\varrho - R_1 \varphi^{\varrho-1} + R_2 \varphi^{\varrho-2} - \ldots \pm R_\varrho = 0,$$

(vergl. § 51) und suchen die Frage zu entscheiden, ob und unter welchen Umständen diese Gleichung eine binomische werden kann; ob es also ϱ-wertige Funktionen giebt, welche, in die ϱ^{te} Potenz erhoben, symmetrisch werden. Für $\varrho = 2$ wissen wir, dass $\sqrt{\Delta} = \varphi$ der Forderung genügt. Um die aufgeworfene Frage allgemein zu erledigen, setzen wir voraus, wir hätten aus der Funktion φ von der verlangten Eigenschaft die etwa darin enthaltenen Faktoren, welche $= \sqrt{\Delta}$ sind, sämtlich herausgezogen; der Quotient sei ψ, und es werde gesetzt

$$\varphi = (\sqrt{\Delta})^{\alpha} . \psi .$$

Dann wird $\psi^{2\varrho}$ symmetrisch werden, da $\varphi^{2\varrho}$ und $\Delta^{\alpha\varrho}$ es sind. Wir setzen daher

$$\psi^{2\varrho} = S_1 .$$

ω sei eine primitive $2\varrho^{\text{te}}$ Einheitswurzel, ψ_1 eine Wurzel der letzteren Gleichung; dann sind alle Wurzeln derselben

$$\psi_1, \ \omega\psi_1, \ \omega^2\psi_1, \ \ldots \ \omega^{2\varrho-1}\psi_1 ,$$

und daraus folgt

$$\Delta_\psi = \psi_1^{n(n-1)}(1-\omega)^2(1-\omega^2)^2 \ldots (\omega^{2\varrho-2} - \omega^{2\varrho-1})^2 .$$

Diese Diskriminante muss nach Lehrsatz XIII) durch Δ teilbar sein, falls nicht ψ selbst schon symmetrisch ist. Die Faktoren mit ω sind von den x unabhängig, also nicht durch Δ teilbar; ψ_1 enthält nach der Voraussetzung nicht mehr den Faktor $\sqrt{\Delta}$; folglich ist ψ_1 symmetrisch und es wird, je nachdem α gerade oder ungerade ist,

$$\varphi = S, \quad \varphi = \sqrt{\Delta} . S .$$

Lehrsatz XVI. Sind die n Elemente $x_1, x_2, \ldots x_n$ von einander unabhängig, so sind die alternierenden Funktionen die einzigen, bei denen eine Potenz symmetrisch wird, ohne dass sie selbst es sind.

§ 58. Wegen der Wichtigkeit dieses Satzes mögen hier noch zwei Beweise desselben folgen, die auf ganz anderen Grundlagen sich aufbauen.

I) Ist ω eine ϱ^{te} primitive Einheitswurzel, so sind

$$\varphi_1, \ \omega\varphi_1, \ \omega^2\varphi_1, \ \ldots \ \omega^{\varrho-1}\varphi_1$$

alle Wurzeln der Gleichung

$$\varphi^{\varrho} - S = 0 ,$$

falls man unter φ_1 irgend eine derselben versteht. Da die ω Konstanten sind, so haben alle Werte von φ dieselbe Gruppe. Diese ist also nach dem Lehrsatze XI) für $n > 4$ entweder die symmetrische

oder die alternierende Gruppe, oder $= 1$. Die beiden ersten Fälle liefern $\varrho = 1, 2$. Im letzteren Falle wäre G_1, die Gruppe von φ_1, gleich 1, also $\varrho = n!$ Wäre σ die Substitution, welche φ_1 in $\omega\varphi_1$ überführt, so würde σ^λ die Substitution sein, welche φ_1 in $\omega^\lambda\varphi_1$ umwandelt. Es müsste daher die Reihe

$$1,\ \sigma,\ \sigma^2,\ \ldots\ \sigma^\lambda,\ \ldots\ \sigma^{n!-1}$$

aus verschiedenen und daher aus allen möglichen Substitutionen bestehen, die mit n Elementen gebildet werden können. Es würde demnach σ eine Substitution des Grades n und der Ordnung $n!$ sein; solche giebt es für $n > 2$ nicht.

Bei $n = 4$ wäre eine sechswertige Funktion denkbar, deren sechste Potenz einwertig ist; die gemeinsame Gruppe dieser sechs Werte wäre

$$G = [1, (x_1x_2)(x_3x_4), (x_1x_3)(x_2x_4), (x_1x_4)(x_2x_3)].$$

Hier müsste es eine Substitution σ gegeben haben, welche φ_1 in $\varphi_1\omega$ überführte und von der sechsten Ordnung wäre. Das ist bei vier Elementen unmöglich.

§ 59. II) Endlich möge noch ein Beweis hier Platz finden, welcher mit den elementarsten Hilfsmitteln auskommt und gleichzeitig zu einer wichtigen Verallgemeinerung des behandelten Satzes führen wird.

Zuerst kann man die Frage beschränken, indem man ϱ als Primzahl voraussetzt. Denn für $\varrho = p.q$ würde aus

$$\varphi^\varrho = S \quad \text{folgen} \quad (\varphi^q)^p = S,$$

so dass es auch eine Funktion φ^q gäbe, bei welcher bereits die p^{te} Potenz symmetrisch wird; p ist dabei ein beliebiger Teiler von ϱ und kann folglich als Primzahlteiler angenommen werden.

Ist nun φ eine Funktion, welche nicht selbst symmetrisch ist, von der aber eine Primzahlpotenz, nämlich die p^{te} Potenz symmetrisch wird, so enthält die Gruppe von φ nicht alle Transpositionen (§ 34); $\sigma = (x_\alpha x_\beta)$ möge den Wert von S_1 in $\varphi_\sigma \frac{1}{1} \varphi_1$ umwandeln. Aus

$$\varphi_{\sigma^p} = \varphi_1{}^p = S$$

folgt dann, wenn ω eine primitive p^{te} Einheitswurzel bedeutet, dass

$$\varphi_\sigma = \omega\varphi_1$$

ist. Wendet man auf diese Gleichung nochmals die Substitution σ an und bedenkt, dass $\sigma^2 = 1$ und also $\varphi_{\sigma^2} = \varphi$ ist, so folgt die neue Gleichung

$$\varphi_1 = \omega\varphi_\sigma;$$

die Multiplikation beider nebst der Division durch $\varphi_1\varphi_\sigma$ liefert

$$\omega^2 = 1$$

und, weil p eine Primzahl ist, $p = 2$ nebst $\varphi = S.\sqrt{\Delta}$.

Es würde sich, nachdem wir wissen, dass nur alternierende Funktionen in eine Primzahlpotenz erhoben einwertig werden können, noch darum handeln, zu untersuchen, ob es Funktionen giebt, die, in eine Primzahlpotenz erhoben, zweiwertig werden.

ψ sei mehrwertig, seine q^{te} Potenz sei zweiwertig; q möge eine Primzahl sein. Dann giebt es eine Cirkularsubstitution dritter Ordnung $\sigma = (x_\alpha x_\beta x_\gamma)$, die nicht in der Gruppe von ψ vorkommt, da diese ja nicht alle Substitutionen dieser Form enthalten kann, ohne die alternierende Gruppe zu werden (§ 35). Es sei also $\psi_\sigma \neq \psi_1$, aber

$$\psi_\sigma{}^q = \psi_1{}^q = S_1 + S_2 . \sqrt{\Delta},$$

da ψ^q als zweiwertige Funktion unter dem Einflusse einer Cirkularsubstitution dritter Ordnung ungeändert bleibt. Es wird daher, wenn ω eine von 1 verschiedene und also primitive q^{te} Einheitswurzel bezeichnet,

$$\psi_\sigma = \omega \psi_1$$

werden. Wendet man auf diese Gleichung die Substitutionen σ und σ^2 an und bedenkt, dass $\sigma^3 = 1$ und $\psi_{\sigma^3} = \psi_1$ ist, so folgt

$$\psi_{\sigma^2} = \omega \psi_\sigma,$$
$$\psi_1 = \omega \psi_{\sigma^2};$$

durch die Multiplikation dieser drei Gleichungen und Wegheben der Funktionalwerte ergiebt sich $\omega^3 = 1$ und $q = 3$.

Wenn wir $n > 4$ voraussetzen, dann kommen in der Gruppe von ψ auch nicht alle Cirkularsubstitutionen fünfter Ordnung vor (zweites Kapitel Lehrsatz X). Ist τ eine der nicht vorkommenden, so wird $\psi_\tau \neq \psi_1$ sein, dagegen

$$\psi_\tau{}^q = \psi_1{}^q = S_1 + S_2 . \sqrt{\Delta}$$

und daher, wenn unter $\bar{\omega}$ eine von 1 verschiedene q^{te} Einheitswurzel verstanden wird,

$$\psi_\tau = \bar{\omega} \psi_1 .$$

Genau wie oben folgt hieraus, da $\tau^5 = 1$ ist,

$$\psi_{\tau^2} = \bar{\omega} \psi_\tau, \quad \psi_{\tau^3} = \bar{\omega}\, \psi_{\tau^2}, \quad \psi_{\tau^4} = \bar{\omega} \psi_{\tau^3}, \quad \psi_1 = \bar{\omega} \psi_{\tau^4},$$

und durch Multiplikation $\bar{\omega}^5 = 1$, $q = 5$.

Dies widerspricht dem ersten Resultate. Also kann n nicht grösser als 4 sein.

Lehrsatz XVII. Ist $n > 4$, so giebt es keine mehrwertige Funktion, von der eine Potenz zweiwertig würde, falls unter ihren Elementen x keine Beziehungen bestehen.

§ 60. Wir führen diese Untersuchungen dadurch zum Abschluss, dass wir für $n \leq 4$ nach der Existenz von Funktionen der angegebenen Eigentümlichkeit fragen.

Der Fall $n=2$ erledigt sich von selbst.

Für $n=3$ nehmen wir eine systematische Aufsuchung etwa vorhandener Funktionen derart vor, dass wir zuerst den Typus

$$\varphi_1 = \alpha x_1^r + \beta x_2^r + \gamma x_3^r$$

zu Grunde legen und versuchen, α, β, γ und r derart zu wählen, dass den Forderungen genügt wird. Wir benutzen dabei den Umstand, dass ein $\sigma=(x_1 x_2 x_3)$ den Wert $\varphi_\sigma = \omega\varphi_1$ $(\omega^3=1)$ aus φ_1 hervorruft. Es würde also

$$\varphi_\sigma = \alpha x_2^r + \beta x_3^r + \gamma x_1^r = \omega(\alpha x_1^r + \beta x_2^r + \gamma x_3^r),$$
$$\gamma = \omega\alpha, \quad \beta = \omega\gamma = \omega^2\alpha, \quad \alpha = \omega\beta = \omega^2\gamma = \omega^3\alpha = \alpha.$$

Diese drei Gleichungen sind für jedes α erfüllbar; sei $\alpha=1$, so wird

$$\varphi = x_1^r + \omega^2 x_2^r + \omega x_3^r$$

eine Funktion der verlangten Art. Dies zeigt auch die wirkliche Ausrechnung.

Es ergiebt sich

$$\varphi^3 = (x_1^{3r} + x_2^{3r} + x_3^{3r}) + 6x_1^r x_2^r x_3^r - \tfrac{3}{2}(x_1^{2r}x_2^r + x_1^{2r}x_3^r + x_2^{2r}x_3^r + \ldots)$$
$$\pm \tfrac{3}{2}\sqrt{-3}\,(x_1^{2r}x_2^r - x_1^{2r}x_3^r + x_2^{2r}x_3^r - x_2^{2r}x_1^r + x_3^{2r}x_1^r - x_3^{2r}x_2^r).$$

Für $r=1$ erhält man eine Vereinfachung dadurch, dass die letzte Klammer den Wert

$$\sqrt{\Delta} = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$$

erlangt, während sie im allgemeinen Falle nur eine rationale Funktion von $\sqrt{\Delta}$ ist. Setzt man, wie es früher geschah,

$$x_1 + x_2 + x_3 = c_1, \quad x_1x_2 + x_2x_3 + x_3x_1 = c_2, \quad x_1x_2x_3 = c_3,$$

so wird für $r=1$

$$\varphi = \tfrac{1}{2}(-2c_1^3 + 9c_1c_2 - 27c_3 \pm 3\sqrt{-3\Delta}).$$

Es sei jetzt $n=4$.

Dass eine Funktion vom Typus $\alpha x_1^r + \beta x_2^r + \gamma x_3^r + \delta x_4^r$, welche in jedem Summanden nur eine Wurzel enthält, nicht der Bedingung genügen kann, für $\sigma=(x_1x_2x_3)$ den Faktor ω anzunehmen, ist ersichtlich.

Wir versuchen, ob wir bei Funktionen von der Form

$$\varphi_1 = \alpha x_1^r x_2^r + \beta x_2^r x_3^r + \gamma x_3^r x_1^r + x_4^r(\alpha_1 x_1^r + \beta_1 x_2^r + \gamma_1 x_3^r)$$

zum Ziele kommen können. Hier enthält jeder Summand zwei der vier Wurzeln. Sollte sich auch bei diesem Typus die Unmöglichkeit herausstellen, dass die Einwirkung von $\sigma=(x_1x_2x_3)$ den Faktor $\omega = \dfrac{-1+\sqrt{-3}}{2}$ hervorruft, so müssten wir zu neuen Funktionenformen

und zwar zu immer komplizierteren übergehen. Wir werden aber schon hier ein positives Resultat erhalten, und zwar schon für $r = 1$. Es wird

$$\varphi_\sigma = \alpha x_2 x_3 + \beta x_3 x_1 + \gamma x_1 x_2 + x_4 (\alpha_1 x_2 + \beta_1 x_3 + \gamma_1 x_1);$$

und aus $\varphi_\sigma = \omega \varphi_1$ folgt die Reihe der Bedingungen:

$$\gamma = \alpha\,\omega, \quad \beta = \gamma\,\omega = \alpha\,\omega^2, \quad \alpha = \beta\,\omega = \gamma\,\omega^2 = \alpha\,\omega^3,$$
$$\gamma_1 = \alpha_1\omega, \quad \beta_1 = \gamma_1\omega = \alpha_1\omega^2, \quad \alpha_1 = \beta_1\omega = \gamma_1\omega^2 = \alpha_1\omega^3,$$

welche sämtlich für $\omega^3 = 1$ erfüllbar sind. Folglich ist

$$\varphi_1 = \alpha (x_1 x_2 + \omega^2 x_2 x_3 + \omega x_3 x_1) + \alpha_1 (x_1 x_4 + \omega^2 x_2 x_4 + \omega x_3 x_4).$$

Es muss aber auch $\tau = (x_1 x_2 x_4)$ die Funktion φ_1 in φ_τ überführen, derart, dass φ_τ gleich dem Produkte aus φ_1 und einer dritten Einheitswurzel ist, da ${\varphi_1}^3 = {\varphi_\tau}^3$. Ob diese gleich ω, ω^2 oder ω^3 werden wird, lässt sich a priori nicht bestimmen. Man hat

$$\varphi_\tau = \alpha x_2 x_4 + \alpha_1 \omega^2 x_4 x_1 + \alpha_1 x_1 x_2 + x_3 (\omega \alpha x_2 + \omega^2 \alpha x_4 + \omega \alpha_1 x_1).$$

Die Glieder aus φ_1 und φ_τ, welche $x_1 x_4$ enthalten, sind bezüglich

$$\alpha_1 x_1 x_4 \quad \text{und} \quad \alpha_1 \omega^2 x_1 x_4;$$

soll φ_1 mit einer dritten Einheitswurzel multipiziert φ_τ werden, so muss diese daher ω^2 sein. Dann folgen weiter aus

$$\varphi_\tau = \omega^2 \varphi$$

durch Vergleichung der Koefficienten von $x_2 x_4$

$$\alpha = (\alpha_1 \omega^2)\,\omega^2 = \alpha_1 \omega, \quad \alpha_1 = \alpha\,\omega^2,$$

also zwei, aber zwei miteinander übereinstimmende Beziehungen. Dieselben wiederholen sich bei den übrigen Koefficienten, und man findet daher, wenn man nach ω anordnet und den Faktor α gleich 1 setzt

$$\varphi_1 = (x_1 x_2 + x_3 x_4) + \omega (x_1 x_3 + x_2 x_4) + \omega^2 (x_1 x_4 + x_2 x_3).$$

Es ist dies eine Kombination der drei Werte einer früher gefundenen Ausnahmefunktion mit der Gruppe

$$G = [1,\ (x_1 x_2)(x_3 x_4),\ (x_1 x_3)(x_2 x_4),\ (x_1 x_4)(x_2 x_3)].$$

Dass ${\varphi_1}^3$ zweiwertig ist, erkennt man, wenn man

$$x_1 x_2 + x_3 x_4 = y_1, \quad x_1 x_3 + x_2 x_4 = y_3, \quad x_1 x_4 + x_2 x_3 = y_2$$

setzt. Dann stimmt φ mit dem für $n = 3$ abgeleiteten Ausdrucke überein; und da y_1, y_2, y_3 die Wurzeln von

$$y^3 - c_2 q^2 + (c_1 c_3 - 4 c_4)\, y - ({c_1}^2 c_4 - 4 c_2 c_4 + {c_3}^2) = 0$$

sind, wo die c die Koefficienten der Gleichung mit den Wurzeln x_1, x_2, x_3, x_4 bedeuten (§ 52), so können wir den oben für $n = 3$ abgeleiteten Ausdruck sofort in eine zweiwertige Funktion der vier x_1, x_2, x_3, x_4 übersetzen, da, gleichfalls nach § 52, die Beziehung $\Delta_y = \Delta_x$ gilt.

Viertes Kapitel.

Transitivität und Primitivität. Einfache und zusammengesetzte Gruppen. Isomorfismus.

§ 61. Wir haben in diesem Kapitel vier Haupteigenschaften von Substitutionengruppen zu besprechen. Die erste derselben knüpft an die Frage an, ob die Elemente, welche in die Gruppe eingehen, mit einander so in Verbindung stehen, dass ein jedes Element durch jedes andere ersetzt werden kann, oder nicht. Es wird z. B. von den Funktionen

$$x_1x_2 + x_3x_4 \quad \text{und} \quad x_1x_2 - x_3x_4$$

die erste für gewisse Substitutionen ungeändert bleiben, welche auf x_1 folgen lassen x_2 oder x_3 oder x_4; die zweite dagegen wird bei keiner Substitution ungeändert bleiben, welche x_3 oder x_4 auf x_1 folgen lässt. Wir definieren: eine Gruppe heisst transitiv, wenn ihre Substitutionen es gestatten, auf ein beliebiges Element x_1 jedes andere Element $x_2, x_3 \ldots x_n$ folgen zu lassen. Daraus ergiebt sich, dass man auf jedes beliebige Element x_i jedes beliebige andere folgen lassen kann, nämlich durch die Aufeinanderfolge der inversen Substitution s^{-1} von $s = (x_1x_i\ldots)\ldots$ und der direkten $t = (x_1x_k\ldots)\ldots$ Solche Gruppen, welche die angegebene Eigenschaft nicht besitzen, heissen intransitiv. Es ist von den beiden Gruppen (den obigen Funktionen entsprechend)

$$G = [1, (x_1x_2)(x_3x_4), (x_1x_3)(x_2x_4), (x_1x_4)(x_2x_3)],$$
$$G_1 = [1, (x_1x_2)(x_3x_4)]$$

die erste transitiv, die zweite intransitiv.

Für Funktionen gelten dieselben Bezeichnungen, transitiv respektive intransitiv, wie für ihre Gruppen.

Die Elemente einer intransitiven Gruppe teilen sich demnach in Systeme von transitiv zusammenhängenden Elementen. So möge es in einer vorgelegten Gruppe Substitutionen geben, welche x_1, $x_2, \ldots x_a$ untereinander verbinden; andere, welche $x_{a+1}, \ldots x_{a+b}$ verbinden u. s. w., aber keine, die auf x_1 etwa $x_{a+1}, \ldots$ folgen lassen, also ein $x_\lambda (\lambda < a)$ und ein $x_\mu (\mu > a)$ in einem Cyklus haben. Die Maximalanzahl der Substitutionen der einzelnen Systeme ist $a!$ bez. $b!, \ldots$ und daher die Maximalanzahl derjenigen der intransitiven Gruppe bei vorgeschriebenem $a, b, \ldots$ gleich $a!\ b! \ldots$ Ist nur n gegeben, so steht von $a, b, \ldots$ lediglich fest, dass $a + b + \ldots = n$ sei. Dann ergiebt sich die Maximalanzahl der Substitutionen einer intransitiven Gruppe aus den Gleichungen

$$(n-1)!\,1! = \frac{n-1}{2}\cdot(n-2)!\,2! > (n-2)!\,2!, \quad n>3,$$

$$(n-2)!\,2! = \frac{n-2}{3}\cdot(n-3)!\,3! > (n-3)!\,3!, \quad n>5,$$

. . . . . .

$$(a+b+c+d\ldots)! > (a+b)!\,(c+d+\ldots)! > a!\,b!\,c!\ldots$$

Lehrsatz I. Die Maximalzahlen für die Ordnungen intransitiver Gruppen sind

$(n-1)!$, $\frac{1}{2}(n-1)!$; $(n-2)!\,2!$, $(n-2)!$; $(n-3)!\,3!$, $(n-3)!\,2!$; ...

Hier beziehen sich die beiden ersten Ordnungszahlen auf die symmetrische und die alternierende Gruppe von $(n-1)$ Elementen; die dritte auf die Kombination der symmetrischen Gruppen von $(n-2)$ und von 2 Elementen; die vierte kann entweder bei der Kombination der alternierenden Gruppe von $(n-2)$ und der symmetrischen von 2 Elementen auftreten, oder bei der symmetrischen Gruppe von $(n-2)$ Elementen, indem die beiden übrigen Elemente sich gar nicht an der Bildung von Substitutionen beteiligen u. s. f.

Die Konstruktion intransitiver Gruppen aus transitiven kann in ihrer Allgemeinheit erst später (§ 90) angegeben werden.

§ 62. Wir wollen jetzt die Substitutionen einer transitiven Gruppe in eine Tabelle einordnen. Die erste Zeile enthalte alle diejenigen Substitutionen, welche das Element x_1 ungeändert lassen und nur diese, und jede nur ein einziges Mal:

$$s_1 = 1, \quad s_2, \quad s_3, \ldots s_m.$$

Dem Begriffe der Transitivität gemäss giebt es eine Substitution σ_2, welche auf x_1 das Element x_2 folgen lässt. Wir bilden als zweite Zeile unserer Tabelle

$$\sigma_2, \quad s_2\sigma_2, \quad s_3\sigma_2, \ldots s_m\sigma_2$$

und beweisen: 1) alle Substitutionen derselben enthalten die Folge x_1x_2; denn s_α lässt x_1 ungeändert, σ_2 führt x_1 in x_2 über, also wird $s_\alpha\sigma_2$ auch x_1 in x_2 überführen; 2) alle Substitutionen, welche x_2 auf x_1 folgen lassen, sind in dieser Zeile enthalten; denn ist τ eine solche, so wird $\tau\sigma_2^{-1}$ das Element x_1 nicht ändern und daher gleich s_λ sein; τ muss $= s_\lambda\sigma_2$ werden; 3) alle Substitutionen dieser Zeile sind von einander verschieden, da aus $s_\alpha\sigma_2 = s_\beta\sigma_2$ durch rechtsseitige Multiplikation mit σ_2^{-1} folgen würde $s_\alpha = s_\beta$; 4) die Substitutionen dieser Zeile sind von denen der ersteren verschieden, da diese x_1 ungeändert lassen, jene nicht.

Wir wählen weiter eine Substitution σ_3, die x_1 in x_3 überführt, und bilden mit ihr

$$\sigma_3, \quad s_2\sigma_3, \quad s_3\sigma_3, \quad \ldots \; s_m\sigma_3.$$

Dann lassen sich von dieser dritten Zeile dieselben Eigenschaften nachweisen, wie von der zweiten. Wir fahren so fort, bis durch n Zeilen alle Substitutionen der Gruppe aufgebraucht sind. So erkennen wir:

Lehrsatz II. Ist m die Anzahl derjenigen Substitutionen einer transitiven Gruppe, welche ein Element x_1 nicht umstellen, so ist die Ordnung r der Gruppe gleich mn, also ein Vielfaches vom Grade der Gruppe.

Eine leicht ersichtliche Erweiterung dieses Satzes ist folgende:

Zusatz. Sind x_a, x_b, x_c, ... willkürliche Elemente einer Gruppe G, ist m die Anzahl der Stellen, in welche die Substitutionen von G die Elemente x_a, x_b, x_c, ... überführen, r' die Ordnung derjenigen Untergruppe von G, welche x_a, x_b, x_c, ... nicht umsetzt, so ist r die Ordnung von G gleich $m.r'$.

G braucht nicht transitiv zu sein; der Beweis ergiebt sich vermittelst der Bildung einer Tabelle, bei der die Substitutionen jeder einzelnen Zeile x_a, x_b, x_c, ... in gleicher Weise umsetzen.

§ 63. Die m Substitutionen, welche x_1 nicht umsetzen, bilden eine Gruppe G_1, welche in G enthalten ist. Diejenige Untergruppe von G, welche das Element x_2 nicht enthält, heisse G_2 u. s. f. bis zur Untergruppe G_n, welche x_n nicht umstellt.

Alle diese Gruppen sind einander ähnlich, denn man hat, wenn die σ_2, σ_3, ... dieselbe Bedeutung haben wie im vorigen Paragraphen,

$$G_1 = \sigma_2 G_2 \sigma_2^{-1} = \sigma_3 G_3 \sigma_3^{-1} = \ldots = \sigma_n G_n \sigma_n^{-1}.$$

Es sind also alle G_α wie G_1, von der Ordnung m; und wenn wir mit $[q]$ die Anzahl derjenigen Substitutionen von G_1 bezeichnen, welche genau q Elemente umstellen, die übrigen $n-1-q$ aber nicht enthalten, so ist $[q]$ auch die entsprechende Zahl für jede der anderen Gruppen G_2, G_3, ... G_n. Aus der Bedeutung des Symbols $[q]$ folgt dann als Identität

$$m = [n-1] + [n-2] + \ldots + [q] + \ldots + [0],$$

wobei $[0] = 1$ ist. G_1, G_2, ... G_n besitzen demnach insgesamt $n[n-1]$ Substitutionen, welche $n-1$ Elemente umstellen; alle diese sind von einander verschieden, da keine Substitution aus G_β, welche nur x_β nicht umsetzt, in irgend einer anderen Gruppe G_γ vorkommen kann.

Anders ist es mit den Substitutionen, welche genau $n-2$ Elemente umstellen: bleiben in einer Substitution x_α und x_β ungeändert, so kommt sie sowohl in G_α unter den $[n-2]$ vor, als auch in G_β. Hier wird also jede Substitution von den $n[n-2]$ vorhandenen doppelt gerechnet, und in G giebt es nur $\frac{n}{2}[n-2]$ verschiedene Substitutionen, welche genau $n-2$ Elemente umstellen. Ebenso kommt jede der $n[q]$ Substitutionen von q Elementen, welche in $G_1, G_2, \ldots G_n$ auftreten und also $n-q$ Elemente ungeändert lassen, in $n-q$ verschiedenen von diesen Gruppen vor und ist also bei allen $n[q]$ Substitutionen in $G_1, G_2, \ldots G_n$ gerade $(n-q)$ mal gezählt; folglich existieren in G nur $\frac{n}{n-q}[q]$ Substitutionen, die genau q Elemente umstellen. Somit ist die Anzahl aller Substitutionen in G, welche weniger als n Elemente umstellen,

$$\frac{n}{1}[n-1]+\frac{n}{2}[n-2]+\ldots+\frac{n}{n-q}[q]+\ldots+\frac{n}{n}[0].$$

Zieht man diese Zahl von derjenigen aller in G enthaltenen Substitutionen ab, so bleibt die Anzahl derjenigen Substitutionen zurück, welche alle n Elemente umstellen. Nun ist nach dem zweiten Lehrsatze

$$r=m.n=n[n-1]+n[n-2]+\ldots+n[q]+\ldots+n[0],$$

also ist die gesuchte Differenz gleich

$$n\left(\tfrac{1}{2}[n-2]+\tfrac{2}{3}[n-3]+\ldots+\frac{n-q-1}{n-q}[q]+\ldots+\frac{n-1}{n}[0]\right).$$

Keiner der Summanden in der Klammer ist negativ, der letzte wird wegen $[0]=1$ gleich $\frac{n-1}{n}$; also ist diese Anzahl $\geq n-1$.

Lehrsatz III. Jede transitive Gruppe hat mindestens $n-1$ Substitutionen, welche alle n Elemente umsetzen. Giebt es mehr als $n-1$ derartige Substitutionen in der transitiven Gruppe, so besitzt dieselbe auch solche, welche weniger als $(n-1)$ Elemente umsetzen.*

§ 64. Wir betrachten eine zweite Gruppe n^{ten} Grades G'; diese habe mit G alle die Substitutionen gemeinsam, durch welche sämtliche n Elemente umgesetzt werden. G' sei gleichzeitig von möglichst niedriger Ordnung; dann ist jede Substitution von G' auch in G enthalten. G' sei endlich auch transitiv; dann gilt der obige Lehrsatz

* C. Jordan: Liouville Journal (2). XVII p. 351.

auch von ihr, und es ist die Anzahl der Substitutionen in ihr, welche alle Elemente umsetzen,

$$n\left(\tfrac{1}{2}[n-2]'+\tfrac{2}{3}[n-3]'+\ldots\frac{n-q-1}{n-q}[q]'+\ldots+\frac{n-1}{n}[0]'\right),$$

falls $[q]'$ für G' dieselbe Bedeutung hat, wie $[q]$ für G. Der Annahme nach stimmt diese Zahl mit der oben ähnlich gebildeten überein. Man hat also

$$\tfrac{1}{2}\{[n-2]-[n-2]'\}+\tfrac{2}{3}\{[n-3]-[n-3]'\}+\ldots$$
$$\ldots+\frac{n-q-1}{n-q}\{[q]-[q]'\}+\ldots=0.$$

Da G' ganz in G enthalten ist, so kann keine der geschweiften Klammern negativ sein; also sind sie sämtlich gleich Null.

Lehrsatz VI. Stimmen zwei transitive Gruppen in denjenigen Substitutionen überein, welche alle Elemente umsetzen, so können sie sich überhaupt nur in denjenigen Substitutionen von einander unterscheiden, welche nur Ein Element ungeändert lassen.

§ 65. Eine Gruppe keisst k-fach transitiv, wenn ihre Substitutionen es erlauben, k beliebige Elemente auf k gegebene folgen zu lassen. Dann kann man, wie sich leicht zeigt, auf k beliebige Elemente k beliebige andere folgen lassen. Natürlich ist hierin der Fall eingeschlossen, dass einige der Elemente ihre Plätze nicht ändern sollen. So muss es in einer vierfach transitiven Gruppe Substitutionen geben, welche x_1 und x_2 ungeändert lassen, x_3 durch x_4 und x_4 durch x_3 ersetzen; die Substitutionen müssen die Form haben $(x_1)(x_2)(x_3x_4)(x_5\ldots)\ldots$, wo über die Verbindung oder das Vorkommen der Elemente $x_5, x_6, \ldots$ keine weiteren Bedingungen bestehen. Ebenso muss diese Gruppe eine Substitution enthalten, welche x_1, x_2, x_3, x_4 ungeändert lässt; dies thut z. B. die identische Substitution 1.

Wir haben im zweiten Kapitel § 37 eine zweifach transitive Gruppe des Grades 5 und der Ordnung 20 gefunden. Sie wurde durch die Kombination der beiden Substitutionen $s=(x_1x_2x_3x_4x_5)$ und $\sigma=(x_2x_3x_5x_4)$ gebildet, und man überzeugt sich leicht, dass wirklich die Überführung jeder Kombination x_α, x_β in jede andere x_γ, x_δ durch eine und auch nur durch eine Substitution jener Gruppe geleistet werden kann.

Dreifach transitiv ist z. B. die alternierende Gruppe von fünf Elementen. Fordert man etwa eine Substitution derselben, welche x_2 ungeändert lassen und auf x_1 und x_5, respektive x_5, x_3 folgen lassen soll, so wird $s=(x_1x_5x_3)$ der Forderung genügen, da diese Substitution aus

einer geraden Anzahl von Transpositionen zusammengesetzt ist. Vierfach transitiv dagegen ist diese Gruppe nicht; denn sonst müsste sie eine Substitution enthalten, welche x_1, x_2, x_3, x_4 in x_1, x_2, x_3, x_5 umwandelt. Dies könnte nur $\sigma = (x_4 x_5)$ sein; das gehört aber nicht der alternierenden Gruppe an.

Allgemeiner können wir beweisen, dass die alternierende Gruppe von n Elementen $(n-2)$-fach transitiv sei. Denn bei den durch die Transitivität erlaubten Forderungen treten entweder $n-2$, oder $n-1$, oder alle n Elemente auf. Im ersteren Falle können die beiden zurückbleibenden Elemente zu einer Transposition τ verbunden werden, und wenn σ eine Substitution ist, welche den $n-2$ Forderungen genügt, so thut es auch $\sigma\tau$; eine der beiden Substitutionen gehört aber zur alternierenden Gruppe.

Treten dagegen im zweiten Falle $n-1$ Elemente in den Forderungen auf, so liefern dieselben, wenn man sie zu Cyklen zusammenschiebt, eine ungeschlossene Reihe. Denn ein geschlossener Cyklus zwischen m Elementen repräsentiert m Folgen und erfüllt m Forderungen; so oft also von den Forderungen durch gegenseitiges Ineinandergreifen der Elemente geschlossene Cyklen gebildet werden, ist die Zahl der verwendeten Elemente gleich derjenigen der befriedigten Forderungen. Tritt nun in unserem Falle eine ungeschlossene Reihe auf, so kann man sie entweder unmittelbar schliessen, oder erst das letzte noch freie Element hinzufügen und sie dann schliessen. Beide Substitutionen erfüllen die Forderungen; die eine derselben gehört der alternierenden Gruppe an (zweites Kapitel Lehrsatz XI).

Alle n Elemente endlich können nur dann in den $n-2$ Forderungen vorkommen, wenn diese zwei ungeschlossene Reihen hervorrufen. Nun kann man von diesen beiden entweder jede für sich schliessen, oder man kann sie aneinander schieben und in eine Klammer zusammenfassen. Beide Substitutionen erfüllen die Forderungen; die eine derselben gehört der alternierenden Gruppe an, genau wie oben. Die alternierende Gruppe von n Elementen ist also mindestens $(n-2)$-fach transitiv; $(n-1)$-fach transitiv kann sie nicht sein, da sie keine Substitution enthält, welch x_1, x_2, ... x_{n-2} ungeändert lässt und x_{n-1} in x_n überführt.

§ 66. Ist G eine k-fach transitive Gruppe, so wird diejenige Untergruppe G' von G, welche x_1 nicht enthält, $(k-1)$-fach transitiv; diejenige Untergruppe G'' von G', welche x_2 nicht enthält, $(k-2)$-fach transitiv sein, u. s. w.; endlich wird die Gruppe $G^{(k-1)}$, welche x_1, x_2, ... x_{k-1} nicht enthält, einfach transitiv werden. Wendet man nun den

Lehrsatz II) der Reihe nach auf $G^{(k-1)}, \ldots G'', G', G$ an, so erhält man den

Lehrsatz V. Die Ordnung r einer k-fach transitiven Gruppe ist gleich $n(n-1)(n-2)\ldots(n-k+1).m$, wo m die Ordnung einer Untergruppe angiebt, welche k Elemente ungeändert lässt. — Die Gruppe besitzt Substitutionen, welche genau n, solche, welche genau $n-1, \ldots n-k+1$ Elemente umsetzen (Lehrsatz III).

§ 67. Diejenigen Substitutionen einer k-fach transitiven Gruppe G, welche nächst der identischen Substitution 1 möglichst wenige Elemente umfassen, mögen genau q derselben umsetzen. Es fragt sich, ob zwischen den beiden Zahlen k und q irgend ein Zusammenhang besteht. Zuerst sei $k \geqq q$, und s eine der Substitutionen geringster Elementenzahl; ihre Form sei $s = (x_1 x_2 \ldots)\ldots(\ldots x_{q-1} x_q)$. Dann giebt es wegen der k-fachen Transitivität von G eine Substitution, welche den $q \leqq k$ Bedingungen genügt

$x_1, x_2, x_3, \ldots x_{q-1}, x_q$ sollen in $x_1, x_2, x_3, \ldots x_{q-1}, x_\varkappa \quad (\varkappa > q)$ übergehen. $\sigma = (x_1)(x_2)\ldots(x_{q-1})(x_q x_\varkappa \ldots)$ sei eine von den Substitutionen der Gruppe G, welche diese Forderungen erfüllen. Dann ist

$$\sigma^{-1} s \sigma = (x_1 x_2 \ldots)\ldots(\ldots x_{q-1} x_\varkappa),$$
$$(\sigma^{-1} s \sigma) s^{-1} = (x_{q-1} x_\varkappa x_q).$$

Da diese Substitution nur drei Elemente enthält, so kann q nicht grösser sein als 3, falls es kleiner als k oder gleich k ist.

Möge zweitens $k < q$ und $s = (x_1 x_2 \ldots)\ldots(\ldots x_{k-1} x_k \ldots)\ldots(\ldots x_q)$ eine derjenigen Substitutionen sein, welche möglichst wenige Elemente enthalten. Wir wählen ein

$$\sigma = (x_1)(x_2)\ldots(x_{k-1})(x_k x_\varkappa \ldots),$$

was wegen der k-fachen Transitivität möglich ist, und nehmen hierin für $x_\varkappa$ ein Element, welches schon in s vorkommt; auch dies ist möglich, da q mindestens gleich $k+1$ ist. Dann wird die Transformierte von s durch σ

$$\sigma^{-1} s \sigma = (x_1 x_2 \ldots)\ldots(\ldots x_{k-1} x_\varkappa \ldots)\ldots$$

sein; sie kann also höchstens $q-k$ neue Elemente gegen s enthalten, da beide Substitutionen in den ersten $k-1$ Elementen mit einander übereinstimmen und das k^{te} der zweiten in der ersten Substitution vorkommt. In dem Produkte $(\sigma^{-1} s \sigma).s^{-1}$ fallen ferner die ersten $k-2$ Elemente fort, so dass in demselben höchstens noch

$$q + (q-k) - (k-2) = 2q - 2k + 2$$

vorkommen. Der Voraussetzung nach darf diese Zahl nicht kleiner sein als q, d. h. es wird

$$q \geq 2k-2,$$

weil sonst das Produkt $(\sigma^{-1}s\sigma).s^{-1}$ weniger als q Elemente enthielte, was der Annahme über s entgegen ist. Wir sehen also:

Lehrsatz VI. Hat eine k-fach transitive Gruppe Substitutionen von weniger als $2k-2$ Elementen, welche von $s_1=1$ verschieden sind, so besitzt sie auch Substitutionen von höchstens drei Elementen.

Etwas Wesentliches sagt der Satz VI) nur für $k>2$ aus. In diesem Falle können wir unter Vorwegnahme der Resultate des folgenden Paragraphen den Zusatz machen:

Zusatz. Enthält eine k-fach transitive Gruppe ($k>2$) Substitutionen, die von der Einheit verschieden sind und nicht mehr als $2k-2$ Elemente umstellen, so ist sie alternierend oder symmetrisch.

Hiermit kombinieren wir die Schlussbemerkung vom Lehrsatz V). Ist G k-fach transitiv, so enthält es Substitutionen von $n-k+1$ Elementen; es ist also $q \leq n-k+1$. Wenn G weder alternierend noch symmetrisch ist, wird $q \geq 2k-2$. Dann ist also $n-k+1 \geq 2k-2$ und $k \leq \frac{n+3}{3}$.

Lehrsatz VII. Ist eine Gruppe des Grades n weder alternierend noch symmetrisch, so kann sie höchstens $\left(\frac{n}{3}+1\right)$-fach transitiv sein.

§ 68. Lehrsatz VIII. Enthält eine zwei- oder mehrfach transitive Gruppe eine Cirkularsubstitution von drei Elementen, so enthält sie die alternierende Gruppe.

Es sei $s=(x_1x_2x_3)$ die vorkommende Substitution von drei Elementen. Da G mindestens zweifach transitiv ist, so giebt es eine Substitution $\sigma=(x_3)(x_1x_4x_\lambda\ldots)$, folglich auch

$$\tau=\sigma^{-1}s\sigma=(x_3x_4x_\mu), \quad \tau^{-1}s\tau=(x_1x_2x_4);$$

ebenso existieren dann

$$(x_1x_2x_5), (x_1x_2x_6), \ldots$$

und aus § 35 folgt die Richtigkeit unseres Satzes.

Lehrsatz IX. Enthält eine zwei- oder mehrfach transitive Gruppe eine Transposition, so ist sie symmetrisch. Der Beweis ist dem eben geführten ähnlich.

Bei einfacher Transitivität gelten die Sätze VIII) und IX) nur unter gewissen Einschränkungen. Folgende Beispiele mögen dies zeigen:

$$G_1 = [1, (x_1x_2)(x_3x_4), (x_1x_3)(x_2x_4), (x_1x_4)(x_2x_3), (x_1x_2), (x_3x_4), (x_1x_3x_2x_4), (x_1x_4x_2x_3)],$$

$$G_2 = \{1, (x_1x_2x_3), (x_4x_5x_6), (x_7x_8x_9), (x_1x_5x_9x_2x_6x_7x_3x_4x_8)\}.$$

Transitiv sind beide Gruppen. Die erste von ihnen enthält eine Substitution von zwei Elementen, ohne symmetrisch, die zweite G_2 eine solche von drei Elementen, ohne alternierend zu sein. Der Beweis für die erste Behauptung folgt aus der Betrachtung der vollständig niedergeschriebenen Gruppe.

§ 69. Einen Beweis für die letzte Behauptung und eine Erklärung dieser Ausnahmen können wir folgendermassen geben. Wählen wir nach Belieben zwei oder mehrere Substitutionen zwischen n Elementen aus, so ist es als sehr wahrscheinlich anzusehen, dass die Gruppe geringster Ordnung, welche diese Substitutionen umfasst, die symmetrische Gruppe der n Elemente werden wird, oder etwa auch die alternierende. Denn wenn die Substitutionen ganz willkürlich gewählt sind, so werden im allgemeinen keine derartigen speziellen Beziehungen zwischen ihnen bestehen, dass durch alle möglichen Kombinationen unter ihnen nur ein Teil aller $n!$ Substitutionen gebildet würde. Am naheliegendsten ist es noch, anzunehmen, dass die Substitutionen, welche herausgegriffen sind, sämtlich aus je einer geraden Anzahl von Transpositionen zusammengesetzt wären; dann gelangte man zur alternierenden Gruppe.

Im allgemeinen können wir daher jede transitive Gruppe, die nicht symmetrisch oder alternierend ist, und jede intransitive Gruppe, welche nicht aus alternierenden oder symmetrischen Teilen besteht, als Ausnahme ansehen. Diese erklärt sich dann so, dass unter den Substitutionen, welche die Gruppe bestimmen, ganz spezielle Beziehungen stattfinden, durch welche der Kreis der durch Kombination zu erzeugenden Substitutionen ein engerer wird.

Derartige Beziehungen finden bei den obigen beiden Gruppen statt, und auf sie haben wir unsere Aufmerksamkeit zu richten. Bei G_1 wie bei G_2 kommen nämlich gewisse Systemeinteilungen unter den Elementen vor, so dass jede Substitution, welche ein Element eines solchen Elementensystems in eins eines anderen Elementensystems überführt, gleichzeitig alle Elemente des ersten in alle Elemente des anderen Systems umwandelt. Es bilden in G_2 die drei Elemententripel x_1, x_2, x_3, ferner x_4, x_5, x_6, endlich x_7, x_8, x_9 je ein solches System. Lässt eine

Substitution x_4 auf x_1 folgen, so wird sie x_2 und x_3 in x_5 und x_6 oder in x_6 und x_5 übergehen lassen; lässt eine Substitution x_1 ungeändert, so kann sie nur x_2 und x_3 ungeändert lassen oder untereinander vertauschen. In der ersten Gruppe G_1 bilden x_1 und x_2 ein solches System und x_3, x_4 das zweite. Jede Substitution dieser Gruppen kann somit dadurch gebildet werden, dass man zuerst die Systeme in gewisser Weise untereinander vertauscht und dann die Elemente jedes einzelnen Systems unter sich umsetzt. Es kann G_2 demnach nicht die Substitution $(x_1x_2)(x_3x_4)$ enthalten; G_2 ist daher nicht alternierend.

Diese Verhältnisse betrachten wir eingehender.

§ 70. Eine einfach transitive Gruppe heisst imprimitiv, wenn ihre Elemente in Systeme von gleich vielen Lettern x_λ derart eingeteilt werden können, dass alle Substitutionen der Gruppe die Elemente eines Systems immer wieder nur durch alle Elemente desselben oder eines und desselben anderen Systems ersetzen. Die Substitutionen der Gruppe können also derart ausgeführt werden, dass man zuerst nur Systemvertauschungen vornimmt, und dann nur Elementenvertauschungen innerhalb jedes einzelnen Systems zulässt.

Ist eine einfach transitive Gruppe nicht imprimitiv, so möge sie primitiv heissen.

Die Potenzen einer Cirkularsubstitution eines Primzahlgrades (oder was dasselbe ist, einer Primzahlordnung) bilden eine primitive Gruppe.

Die Potenzen einer Cirkularsubstitution von zusammengesetztem Grade bilden eine imprimitive Gruppe. Die Systeme der Elemente können hierbei stets auf mehrere verschiedene Weisen gewählt werden. So kann man bei

$$G = [1, (x_1x_2x_3x_4x_5x_6), (x_1x_3x_5)(x_2x_4x_6), (x_1x_4)(x_2x_5)(x_3x_6),$$
$$(x_1x_5x_3)(x_2x_4x_6), (x_1x_6x_5x_4x_3x_2)]$$

entweder zwei Systeme von je drei Elementen bilden x_1, x_3, x_5 und x_2, x_4, x_6, oder drei Systeme von je zwei Elementen x_1, x_4, dann x_2, x_5 und endlich x_3, x_6. Es gilt hier der Satz, dessen Beweis wir seiner Einfachheit halber übergehen können:

Lehrsatz X. Ist bei einer imprimitiven Gruppe die Einteilung der Elemente in Systeme auf zweierlei Art möglich, so kann man eine dritte Einteilung dadurch herleiten, dass man alle Elemente, welche ein System der ersten mit einem Systeme der zweiten Einteilung gemeinsam hat, zu einem neuen Systeme der dritten Einteilung vereinigt.

Zu beachten ist dabei nur, dass ein einziges Element kein System in unserem Sinne zu konstituieren im Stande ist.

§ 71. Wir können die Substitutionen einer imprimitiven Gruppe folgendermassen in eine Tabelle einreihen. Die erste Zeile enthält alle und nur diejenigen Substitutionen, welche die einzelnen Systeme ungeändert lassen und also nur die Elemente innerhalb eines jeden Systems vertauschen dürfen. (Je nach der Wahl der zu Grunde gelegten Einteilung in Systeme kann diese Zeile verschieden ausfallen.)

Wir bezeichnen die darin vorkommenden Substitutionen durch

$$s_1 = 1,\ s_2,\ s_3,\ \ldots\ s_m.$$

Dem Begriffe der Transitivität gemäss (denn Primitivität und Imprimitivität bestehen nur bei einfach transitiven Gruppen) giebt es eine Substitution σ_2, welche ein Element eines Systems in ein solches eines andern und damit die Systeme überhaupt in gewisser Art untereinander vertauscht. Wir bilden als zweite Zeile

$$\sigma_2,\ s_2\sigma_2,\ s_3\sigma_2,\ \ldots\ s_m\sigma_2$$

und beweisen: 1) alle Substitutionen dieser zweiten Zeile lassen die Systeme in derselben Weise aufeinander folgen wie σ_2; denn jedes s_α lässt sie ja ungeändert; 2) alle Substitutionen, welche die Systeme so aufeinander folgen lassen wie σ_2, stehen in dieser Zeile; denn thut es τ, so wird $\tau\sigma_2^{-1}$ die Systeme nicht ändern, demnach $= s_\alpha$ sein und τ wird $= s_\alpha\sigma_2$; 3) alle Substitutionen der zweiten Zeile sind von einander verschieden, und 4) von denen der ersten Zeile.

Giebt es eine neue Substitution σ_3, welche eine andere Vertauschung der Systeme nach sich zieht, so giebt sie die Veranlassung zur Bildung einer dritten Zeile, von welcher sich dieselben Eigenschaften nachweisen lassen u. s. w.

Lehrsatz XI. Besitzt die imprimitive Gruppe G eine Untergruppe G_1 von der Ordnung m, welche die einzelnen Systeme nicht untereinander vertauscht, so ist die Ordnung r von G gleich $m.q$. Dabei bedeutet q einen Teiler von $\mu!$, μ die Anzahl der Systeme.

§ 72. Wir betrachten die Ordnung m von G_1 etwas genauer. Da G_1 kein Element eines Systems in ein Element eines anderen überführen darf, so ist es intransitiv. Die Anzahl der einzelnen transitiv untereinander verbundenen Elemente ist gleich der Anzahl der Elemente der Systeme, also für jedes x_i dieselbe und zwar ein Teiler von n. Es sei t eine beliebige Substitution von G; dann bilden wir

$$t^{-1}G_1t^{+1}.$$

Das Resultat ist eine Untergruppe von G, welche G_1 ähnlich ist und die Systeme nicht mit einander vertauscht; es ist also G_1 selbst. Be-

trachten wir jetzt aus G_1 nur diejenigen Bestandteile der Substitutionen, welche die Elemente des ersten Systems der Imprimitivität unter einander vertauschen, so bilden diese eine Gruppe H_1; ebenso mögen die Bestandteile der einzelnen Substitutionen von G_1, welche die Elemente des α^{ten} Systems der Imprimitivität enthalten, die Gruppe H_α bilden. H_1 und H_α sind einander ähnlich. Denn wenn x'_1 ein Element des ersten, $x_1^{(\alpha)}$ ein Element des α^{ten} Systems der Imprimitivität ist, dann giebt es in der transitiven Gruppe G eine Substitution t, welche $x_1^{(\alpha)}$ auf x'_1 folgen lässt, und damit alle Elemente des α^{ten} auf die des ersten Systems. $t^{-1}G_1t$ wandelt folglich die Bestandteile der Substitutionen von G_1 so um, dass die Gruppe H_1 in H_α transformiert wird. H_1 und H_α sind einander demnach ähnlich; die Ordnung des H bezeichnen wir mit r'.

Existieren μ Systeme der Imprimitivität und daher μ Gruppen $H_1, H_2, \ldots H_\mu$, so wird G_1 eine Untergruppe von

$$\Gamma = \{H_1, H_2, \ldots H_\mu\}$$

werden. Γ hat die Ordnung r'^μ; die Ordnung von G_1 ist ein Teiler hiervon.

Lehrsatz XII. Besitzt die nicht primitive Gruppe G μ Systeme der Imprimitivität, so ist die Ordnung r von G ein Teiler von $\mu! \left(\frac{n}{\mu}!\right)^\mu$. Die Ordnung einer imprimitiven Gruppe des Grades n hat als Maximalzahlen ihrer Ordnung

$$2\left(\frac{n}{2}!\right)^2, \quad 3!\left(\frac{n}{3}!\right)^3, \quad 3\cdot\left(\frac{n}{3}!\right)^3, \cdots$$

§ 73. Hinsichtlich der Konstruktion imprimitiver Gruppen können wir folgendes aussagen. Wir wählen eine beliebige Gruppe von $\frac{n}{\mu}$ Elementen $x'_1, x'_2, x'_3, \ldots$, welche H_1 heissen mögen; ihre Ordnung sei r'. Aus $\mu - 1$ anderen Systemen von Elementen $x''_1, x''_2, x''_3, \ldots$; $x'''_1, x'''_2, x'''_3, \ldots$ werden $\mu - 1$ neue Gruppen $H_2, H_3, \ldots H_\mu$ gebildet, welche sämtlich dem H_1 ähnlich sind. Endlich seien $s_1^{(\alpha)}, s_2^{(\alpha)}, \ldots$ die Substitutionen von H_α und

$$\Gamma = \{H_1, H_2, \ldots H_\mu\}.$$

Die Ordnung der intransitiven Gruppe Γ ist r'^μ.

Aus μ anderen Elementen $y_1, y_2, \ldots y_\mu$ werde jetzt weiter eine beliebige transitive Gruppe K konstruiert; ihre Ordnung sei r_1; ihre Substitutionen mögen $t_1, t_2, \ldots t_{r_1}$ heissen. Dann ist

$$G = \{\Gamma, K\}$$

eine intransitive Gruppe aus $n+\mu$ Elementen. Wir wollen aber in dem Ausdrucke von G die Substitutionen von K symbolisch auffassen: Die Umstellung der Elemente $y_1, y_2, \ldots y_\mu$ soll durch die entsprechende Vertauschung der oberen Indices der $x'_1, x'_2, \ldots x''_1, x''_2, \ldots$ ersetzt werden. Ist z. B.

$$s'_1 = 1, \quad t_1 = (y_1 y_2 y_3), \quad \text{so wird} \quad s'_1 t_1 = (x'_1 x''_1 x'''_1)(x'_2 x''_2 x'''_2)\ldots,$$

indem $s'_1 = (x'_1)(x'_2)(x'_3)\ldots$ das Element x'_1 ungeändert lässt, t_1 aber den oberen Index verschiebt u. s. f.; ebenso wird für

$$s'_2 = (x'_1 x'_2 x'_3), \quad s''_3 = (x''_1 x''_2), \quad t_2 = (y_1 y_2),$$
$$s'_2 s''_3 t_2 = (x'_1 x''_2)(x'_2 x''_3 x'_3 x''_1)$$

werden, wie leicht ersichtlich ist u. s. f.

Unter dieser Voraussetzung wird G eine imprimitive Gruppe von n Elementen, die sich in μ Systeme der Imprimitivität verteilen. Die Ordnung derselben ist $r = r'^{\mu} . r_1$.

Dies folgt daraus, dass

$$t_\lambda^{-1} \Gamma t_\lambda = \Gamma$$

wird, so dass es nur r'^{μ} Substitutionen giebt, welche die Systeme nicht umstellen, und r_1 verschiedene Systemfolgen, gemäss den r_1 Substitutionen t_λ von K.

Wenn umgekehrt eine imprimitive Gruppe gegeben ist, und σ_ϑ bedeutet eine Substitution derselben, so kann man aus μ neuen Elementen $y_1, y_2, \ldots y_\mu$ eine Substitution t_ϑ konstruieren, welche die y so umsetzt, wie σ_ϑ die Systeme. Verfährt man so bei allen Substitutionen der Gruppe, dann erhält man ein System $t_1, t_2, \ldots$; diese bilden eine transitive Gruppe. Alle $\sigma_\vartheta t_\vartheta^{-1}$ liefern, symbolisch aufgefasst, Substitutionen, welche die Systeme nicht mehr vertauschen; sie bilden eine intransitive Gruppe Γ_1, bei der die einzelnen Systeme intransitiver Elemente gleich gross sind. Γ_1 hat die Eigenschaft, sich bei der Operation $t_\lambda^{-1} \Gamma_1 t_\lambda$ zu reproduzieren. Dies reicht hin, um von ihr aus zu G zu gelangen. Die oben angegebene Konstruktion von Γ ist also nicht allgemein genug; doch sind in der nach jener Vorschrift konstruierten Gruppe G alle imprimitiven Gruppen von n Elementen mit μ Systemen der Imprimitivität enthalten.

§ 74. Jetzt wollen wir den Einfluss untersuchen, den die Primitivität auf eine transitive Gruppe ausübt. Wir knüpfen dabei an die Lehrsätze VIII) und IX) dieses Kapitels an, indem wir, in gewissem Sinne jene erweiternd, den Satz aufstellen:

Lehrsatz XIII. Enthält eine primitive Gruppe eine der beiden Substitutionen

$$\sigma = (x_1 x_2 x_3) \quad \text{oder} \quad \tau = (x_1 x_2),$$

so umfasst sie im ersten Falle die alternierende, im zweiten die symmetrische Gruppe.

Wir werden diesen Satz als einen Spezialfall des folgenden ansehen und beweisen:

Lehrsatz XIV. Enthält eine primitive Gruppe eine Cirkularsubstitution s der Primzahlordnung p, so enthält sie eine Reihe ähnlicher Substitutionen

$$s_1, s_2, s_3, \ldots s_\lambda, \ldots s_{n-p+1}$$

derart, dass s_λ die Elemente $x_1, x_2, x_3, \ldots x_{p-1}; x_{p+\lambda-1}$ enthält. Dabei können $x_1, x_2, \ldots x_{p-1}$ beliebig gewählt werden.

Gemäss Kapitel 2 Lehrsatz VI) und IX) erhält man dann für $p = 2, 3$ aus dem letzten Satze den darüberstehenden.

Wir wenden uns zum Beweise von Lehrsatz XIV).

Die primitive Gruppe G soll eine Substitution s enthalten, welche durch einen einzigen Cyklus von der Primzahlordnung p gebildet wird. Wir transformieren s durch alle Substitutionen der Gruppe und erhalten dadurch eine Reihe ähnlicher Substitutionen $s, s', s'', \ldots s^{(\nu)}, \ldots$ Diese setzen bereits alle Elemente von G miteinander in Verbindung, so dass $H = \{s, s', \ldots s^{(\nu)}, \ldots\}$ transitiv ist. Denn wäre dies nicht der Fall, dann mögen $x_1, \ldots x_k$ alle die Elemente sein, welche in H mit dem Elemente x_1 verbunden auftreten, während ξ_1 ein neues Element sein soll. Transformiert man nun $s, s', s'', \ldots$ durch eine der Substitutionen, welche auf ein x_λ folgen lassen ξ_1, so wird dadurch an Stelle von x_λ das neue Element ξ_1 treten. Soll dies nicht mit den früheren in Verbindung stehen, so müssen gleichzeitig alle $x_1, x_2, \ldots x_k$ durch neue Elemente $\xi_1, \xi_2, \ldots \xi_k$ ersetzt werden. Erschöpfen die x_λ und die ξ_λ noch nicht alle vorhandenen Elemente derart, dass etwa noch ein η_1 vorkommt, so giebt es eine Substitution, welche x_1 durch η_1 ersetzt; denn G ist transitiv. Transformiert man $s, s', s'', \ldots$ durch diese Substitution, so geht H in sich, alle x_λ gehen in neue Elemente über $\eta_1, \eta_2, \ldots \eta_k$. Diese sind sämtlich von den ξ_λ verschieden; denn wäre dies nicht der Fall, so würden mehr als k Elemente $\xi_1, \xi_2, \ldots \xi_k, \eta_1, \eta_\alpha, \eta_\beta, \ldots$ durch $s, s', s'', \ldots$ in Verbindung stehen; transformierte man nun durch den reciproken Wert einer Substitution, welche alle x_λ in alle ξ_λ überführt, so würden die $\eta_1, \eta_\alpha, \eta_\beta, \ldots$ in Elemente umgewandelt werden, welche auch noch mit den x_λ in Verbindung ständen; das ist nicht möglich. So kann man weitergehen und erkennt, dass aus unserer Annahme die Imprimitivität von

G folgen würde. Demnach hängen durch s, s', s'', ... $s^{(\nu)}$, ... bereits alle Elemente der Gruppe zusammen.

Wir greifen jetzt aus der Reihe s', s'', s''', ... eine Substitution heraus, welche einige Elemente mit s gemeinsam hat und andere neue mit denen von s in Verbindung setzt. Nach der obigen Überlegung giebt es derartige Substitutionen; s' sei eine solche. Sollten nun in dem Cyklus von s' mehrere neue Elemente auftreten, so kann man in einer passend gewählten Potenz s'^{α} zwei von diesen aufeinander folgen lassen. In $s'^{-\alpha} s s'^{\alpha}$ wird dann, wie man leicht erkennt, das zweite der neuen Elemente und überhaupt jedes neue, welches auf ein anderes neues folgt, wegfallen; dagegen jedes neue, welches auf ein altes folgt, bleiben; die Transformierte $s'^{-\alpha} s s'^{\alpha}$ hat somit auch noch neue Elemente mit denen von s in Verbindung gebracht, aber weniger als s'. Ist etwa

$$s' = (x_1 x_a x_2 x_b x_3 x_6 x_c x_5 x_9), \quad s = (x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8 x_9),$$

so wird

$$s'^2 = (x_1 x_2 x_3 x_c x_9 x_a x_b x_6 x_5), \quad s'^{-2} s s'^2 = (x_1 x_5 x_7 x_8 x_a x_2 x_3 x_c x_4) = t.$$

Enthält die Transformierte noch immer mehr als ein neues Element, so kann man nach derselben Methode fortfahren, bis man auf eine Substitution gekommen ist, welche $p-1$ Elemente mit s gemeinsam hat und nur ein neues enthält. Im obigen Beispiel wäre zu nehmen

$$t^3 = (x_1 x_8 x_3)(x_2 x_4 x_7)(x_5 x_a x_c), \quad t^{-3} s t^3 = (x_1 x_7 x_a x_6 x_2 x_3 x_9 x_8 x_4).$$

(Es ist hier absichtlich die Ordnung von s gleich 9 gewählt worden, um zu zeigen, dass die Ordnung, wie unser Lehrsatz es voraussetzt, eine Primzahl sein muss. Denn t^3 zerfällt hier in drei Cyklen, und es hätte leicht eintreten können, dass einige dieser Cyklen nur fremde, alle andern nur frühere Elemente enthalten hätten; dann würde eine Transformation zu nichts geführt haben.)

$s = s_1$ möge die Elemente x_1, x_2, ... x_{p-1}, x_p und die neu konstruierte Substitution, welche s_2 heissen mag, die Elemente x_1, x_1, ... x_{p-1}, x_{p+1} enthalten. Man kann in derselben Weise weiter fortfahren, indem man eine neue Substitution bestimmt, welche mit den Elementen von s_1 oder s_2 neue verbindet. Es möge z. B. s'_1 mit s_1 die $p-1$ Elemente x_2, x_3, ... x_{p-1}, x_p gemeinsam haben und das neue Element x_{p+2} einführen. Nimmt man dann s'^{α}_1 so, dass in dieser Potenz x_p auf x_{p+2} folgt, und bildet man $s'^{-\alpha}_1 s_1 s'^{\alpha}_1$, so wird in dieser Transformierten das Element x_p weggefallen sein. Man erhält also, wenn diese Substitution s_3 benannt wird,

s_1 mit den Elementen $x_1, x_2, \ldots x_{p-1}; x_p,$
s_2 „ „ „ $x_1, x_2, \ldots x_{p-1}; x_{p+1},$
s_3 „ „ „ $x_1, x_2, \ldots x_{p-1}; x_{p+2},$

und kann so fortgehen, bis alle Elemente erlangt sind.

Es bleibt noch der Beweis für den letzten Teil des Satzes zu führen, dass die Wahl von $x_1, x_2, \ldots x_{p-1}$ eine willkürliche ist. Jedenfalls enthält eine Substitution σ_1 der Reihe $s_1, s_2, s_3, \ldots$ eins der verlangten Elemente. Diese wähle man zum Ausgangspunkt einer Reihe $\sigma_1, \sigma_2, \sigma_3, \ldots$, bei welcher das geforderte Element in allen σ auftritt. Eine der Substitutionen τ_1 der Reihe $\sigma_1, \sigma_2, \sigma_3, \ldots$ enthält ausser diesem ein zweites der vorgeschriebenen Elemente; τ_1 wähle man zum Ausgangspunkt einer neuen Reihe $\tau_1, \tau_2, \tau_3, \ldots$, welche in jeder Substitution bereits zwei der verlangten Elemante hat. So gehe man fort, bis alle $p-1$ vorgeschriebenen Elemente erhalten worden sind.

§ 75. Lehrsatz XV. Enthält eine primitive Gruppe eine Cirkularsubstitution der Primzahlordnung p, so ist sie mindestens $(n-p+1)$-fach transitiv.

Durch diesen Satz wird der Einfluss des Mangels der Imprimitivität auf transitive Gruppen klar gelegt; Imprimitivität ist eine Eigenschaft einer Gruppe; Primitivität ist nur der Mangel derselben, welcher der Gruppe dadurch einen allgemeinen Charakter verleiht, dass er spezielle Beziehungen ausschliesst.

Es seien s_1, s_2 die beiden im vorigen Paragraphen abgeleiteten Substitutionen. Diese bilden eine zweifach transitive Gruppe. Denn ist zuerst die Folge $x_a x_b x_d$ gefordert, wo x_d auch $= x_a$ sein kann, dann leiten wir aus s_1, s_2 durch Transformationen zwei Substitutionen σ_1, σ_2 ab, von denen die erste beide Elemente x_a, x_b enthält, während in der zweiten x_b nicht vorkommt. Nun sei $\sigma_1{}^\alpha = (x_a x_b x_c \ldots)$, dann bestimmen wir $\sigma_2{}^\beta = (x_c x_d \ldots)$ und bilden $\sigma_1{}^\alpha \sigma_2{}^\beta = \ldots x_a x_b x_d \ldots$ Sollte x_c in $\sigma_1{}^\alpha$ schon $= x_d$ sein, so wird $\beta = 0$.

Ist zweitens $x_a x_b$, $x_d x_e$ gemäss der zweifachen Transitivität gefordert, so wählt man σ_3 so, dass es x_d nicht enthält, σ_2 wie soeben; dann wird $\sigma_3{}^\gamma = (x_a x_b \ldots)$, $\sigma_2{}^\varepsilon = (x_d x_e \ldots)$ und $\sigma_3{}^\gamma . \sigma_2{}^\varepsilon = \ldots x_a x_b \ldots x_d x_e \ldots$ werden.

Ebenso lässt sich zeigen, dass die aus s_1, s_2, s_3 gebildete Gruppe dreifach transitiv wird. Wird nämlich gefordert, dass die Folgen $x_a x_b$, $x_c x_d$, $x_e x_f$ in einer Substitution vorkommen, so konstruiert man aus s_1, s_2, s_3 durch Transformationen σ_1, σ_2, σ_3 so, dass σ_3 weder x_b noch x_d enthält, während x_a, x_b; x_c, x_d in σ_1, σ_2 vorkommen. Dann

kann man in der aus σ_1, σ_2 gebildeten zweifach transitiven Gruppe die Folgen $x_a x_b$ und $x_c x_d$ in einer Substitution hervorrufen; durch eine geeignete Potenz von σ_3, welche dieser Substitution angefügt wird, ändern sich diese Folgen nicht und $x_e x_f$ tritt hinzu.

So geht es in gleicher Weise weiter; da $n-p+1$ Substitutionen vorhanden sind, so folgt der ausgesprochene Satz.

Wir kombinieren dieses Resultat mit demjenigen von § 67 Lehrsatz VII). Dort zeigte sich, dass der Index der Transitivität k den Wert $\frac{n}{3}+1$ nicht überschreiten kann, ohne dass die Gruppe alternierend oder symmetrisch wird. Da nun eine Cirkularsubstitution von p Elementen bei einer primitiven Gruppe $k \geqq n-p+1$ hervorruft, so würde aus $n-p+1 \geqq \frac{n}{3}+1$ oder $p \leqq \frac{2n}{3}$ folgen, dass die gegebene Gruppe die alternierende in sich schliesst. Man erkennt also:

Lehrsatz XVI. Enthält eine transitive Gruppe des Grades n eine Cirkularsubstitution der Primzahlordnung $p < \frac{2n}{3}$, ohne dass sie die alternierende Gruppe enthält, so ist sie imprimitiv.

§ 76. Wir können den Gang des Beweises aus dem vorigen Paragraphen benutzen, um den folgenden, dem Lehrsatze XV) verwandten Satz zu beweisen:

Lehrsatz XVII. Enthält eine primitive Gruppe des Grades n eine $k(\geqq 2)$-fach transitive Untergruppe des Grades q, so ist die erstere Gruppe mindestens $(n-q+k)$-fach transitiv.

Ist G_1 die k-fach transitive Untergruppe des Grades q mit den q Elementen $x_1, x_2, \ldots x_{q-1}, x_q$, so können wir durch Transformation von G_1 durch alle Substitutionen von G eine Reihe von Gruppen ableiten, die dem G_1 ähnlich sind und so beschaffen sein werden, dass $\Gamma = \{G_1, G_2, \ldots\}$ bereits alle Elemente in Verbindung bringt. Denn wäre dies nicht der Fall, so könnte man wie oben die Imprimitivität von G beweisen. Ferner lässt sich zeigen, dass man der Gruppe G_α die Elemente $x_1, x_2, \ldots x_{q-1}, x_{q+\alpha-1}$ geben kann.

Ist nun G_1 eine k-fach transitive Gruppe, so wird $\{G_1, G_2\}$ mindestens $(k+1)$-fach transitiv, wie die obige Beweisführung ergiebt; $\{G_1, G_2, G_3\}$ mindestens $(k+2)$-fach transitiv u. s. f., bis man zur $(n-q+k)$-fachen Transitivität der Gruppe G selbst gelangt.

§ 77. Wir haben in § 71 eine Tabelle entworfen, in welcher die Substitutionen einer imprimitiven Gruppe untergebracht waren. Die

erste Zeile enthielt diejenigen Substitutionen derselben, welche die einzelnen Systeme der Imprimitivität nicht mit einander verband und also nur die Elemente jedes Systems unter sich vertauschte. Diese Substitutionen bildeten daher eine Untergruppe G_1 von G. Von dieser Untergruppe G_1 haben wir eine wichtige Eigenschaft nachgewiesen. Es zeigte sich, dass $t^{-1}G_1t^{+1}=G_1$ wird; dass sich also G_1 bei der Transformation durch eine beliebige Substitution t von G reproduziert. Wir können dies auch durch die Schreibweise $G^{-1}G_1G=G_1$ oder $G_1G=GG_1$ ausdrücken, wobei aber hervorzuheben ist, dass diese nur eine Eigenschaft von G_1, aber nicht eine solche von G aussagt; denn es ist selbstverständlich, dass $G_1^{-1}GG_1=G$ ist, da alle Substitutionen der linken Seite in G enthalten sind.

Wir machen nun im Anschluss an diese Bemerkungen folgende Festsetzungen: Wir nennen

1) s_1, s_2 vertauschbar, wenn $s_1.s_2=s_2.s_1$ ist;
2) s_1 mit H vertauschbar, wenn $s_1H=Hs_1$ ist;
3) H mit G vertauschbar, wenn $H.G=G.H$ ist.

Sollte im letzten Falle H eine Untergruppe von G sein, so drückt die Gleichung $H.G=G.H$ nur eine Eigenschaft von H aus. Wir nennen H dann eine ausgezeichnete Untergruppe von G.

Als Beispiele hierfür mögen gelten:

1) $(x_1x_2x_3x_4)$ ist mit $(x_1x_3)(x_2x_4)$ vertauschbar; jede Potenz s^α einer Substitution ist mit jeder anderen Potenz s^β derselben Substitution vertauschbar.

2) $H=[1, (x_1x_2)(x_3x_4), (x_1x_3)(x_2x_4), (x_1x_4)(x_2x_3)]$ ist mit jeder Substitution der vier Elemente x_1, x_2, x_3, x_4 vertauschbar; die alternierende Gruppe von n Elementen ist mit jeder Substitution derselben Elemente vertauschbar.

3) H ist mit der symmetrischen Gruppe der vier Elemente x_1, x_2, x_3, x_4 vertauschbar; die alternierende Gruppe von n Elementen ist mit der symmetrischen vertauschbar; oder, die alternierende ist eine ausgezeichnete Untergruppe der symmetrischen.

§ 78. Mit diesen Festsetzungen können wir auf ein im zweiten Kapitel behandeltes Thema, auf die Bildung von Substitutionengruppen zurückgreifen (§§ 37, 38).

Alle Substitutionen von n Elementen, die mit einer gegebenen Substitution derselben Elemente vertauschbar sind, bilden eine Gruppe. Denn wenn man hat

$$t_1^{-1} u t_1 = u, \quad t_2^{-1} u t_2 = u,$$

dann folgt daraus, dass auch

$$(t_1 t_2)^{-1} . u . (t_1 t_2) = t_2^{-1} [t_1^{-1} u t_1] t_2 = u$$

wird, so dass sich auch $t_1 . t_2$ unter dem Substitutionenkomplex findet.

Alle Substitutionen von n Elementen, die mit einer gegebenen Gruppe derselben Elemente vertauschbar sind, bilden eine Gruppe, welcher die gegebene als ausgezeichnete Untergruppe angehört.

Denn aus

$$t_1^{-1} G t_1 = G, \quad t_2^{-1} G t_2 = G$$

folgt

$$(t_1 t_2)^{-1} G (t_1 t_2) = G.$$

Enthalten zwei Gruppen G und H ausser der Einheit keine gemeinsamen Substitutionen, und sind G und H mit einander vertauschbar, so wird die Minimalgruppe

$$K = \{G, H\}$$

als Ordnung das Produkt der Ordnungen von G und von H besitzen.

§ 79. Eine ausgezeichnete Untergruppe einer transitiven Gruppe enthält alle Elemente derselben. Denn wäre $H = G^{-1} H G$ eine ausgezeichnete Untergruppe der transitiven Gruppe G, enthielte H das Element x_1 nicht, und führte s_λ aus G dieses Element nach x_λ, so enthielte $s_\lambda^{-1} H s_\lambda$ an Stelle von x_1 jetzt nicht mehr x_λ; da aber jene Transformierte $= H$ ist, so enthielte H weder x_1 noch x_λ, d. h. überhaupt kein Element, da der Index λ beliebig ist.

Ist eine ausgezeichnete Untergruppe H einer transitiven Gruppe G intransitiv, so ist G imprimitiv und H verbindet nur die Elemente der einzelnen Systeme der Imprimitivität unter sich. Denn gehört x_1 einem Systeme der Intransitivität in H an, x_λ einem zweiten und ist s_λ eine Substitution aus G, welche x_λ auf x_1 folgen lässt, so wird $s_\lambda^{-1} H s_\lambda$ an die Stelle von x_1 das Element x_λ setzen und an die Stelle aller mit x_1 transitiv verbundenen alle, welche durch H mit x_λ transitiv zusammenhängen. Da jene transformierte Gruppe $= H$ ist, so erkennt man die Richtigkeit des Ausspruches.*

§ 80. Besitzt G eine ausgezeichnete Untergruppe H, die von der Einheit verschieden ist, so heisst G zusammengesetzt; findet dies nicht statt, so heisst G einfach. Existiert neben H keine ausgezeichnete Untergruppe K von G, von welcher H Untergruppe ist, so heisst H eine ausgezeichnete Maximaluntergruppe.

* Vergl. das Verhältnis von Γ und G in § 76.

Ist G zusammengesetzt und die Reihe der Gruppen

$$G,\ G_1,\ G_2,\ \dots\ G_\mu,\ 1$$

so beschaffen, dass jede folgende Gruppe eine ausgezeichnete Maximaluntergruppe der vorhergehenden ist, so heisst diese Reihe die zur zusammengesetzten Gruppe G gehörige Reihe, oder auch die Reihe der Zusammensetzung von G, respektive kurz die Reihe von G.

Sind die Zahlen

$$r,\quad r_1=\frac{r}{e_1},\quad r_2=\frac{r_1}{e_2},\ \dots\ r_\mu=\frac{r_{\mu-1}}{e_\mu},\quad r_{\mu+1}=\frac{r_\mu}{e_{\mu+1}}=1$$

die Ordnungen der entsprechenden Gruppen der Reihe, so heissen e_1, e_2, $\dots\ e_{\mu+1}$ die Faktoren der Zusammensetzung von G oder auch die Zahlenfaktoren der Zusammensetzung von G. Es wird $r=e_1e_2\dots e_{\mu+1}$.

§ 81. Möglicherweise ist, wenn die zusammengesetzte Gruppe G vorliegt, die Reihe der Zusammensetzung für dieselbe keine unbedingt bestimmte. Es wäre denkbar, dass ausser der angeführten noch andere Reihen, z. B.

$$G,\ G'_1,\ G'_2,\ G'_3,\ \dots\ G'_\nu,\ 1$$

beständen, so dass auch hier jede Gruppe eine ausgezeichnete Maximaluntergruppe der voraufgehenden wäre. Es wird sich zeigen, dass, wie die Reihe auch immer gewählt werden möge, die Faktoren der Zusammensetzung stets dieselben sein werden, abgesehen von ihrer Reihenfolge; dann muss natürlich auch $\mu=\nu$ sich herausstellen.

G_1 enthalte die Substitutionen s_α, G'_1 enthalte die Substitutionen s'_α; $r_1=\frac{r}{e_1}$ sei die Ordnung von G_1, $r'_1=\frac{r}{e'_1}$ die von G'_1. Die Substitutionen, welche G_1 und G'_1 gemein haben, bilden eine Gruppe Γ (drittes Kapitel § 44); die Ordnung x derselben ist ein Teiler von r_1 und von r'_1; wir setzen $r_1=xy,\ r'_1=xy'$.

Die Substitutionen von Γ seien σ_α. Dann kann man alle Substitutionen von G_1 in einer Tabelle von y Zeilen unterbringen, deren erste alle Substitutionen σ_α von Γ enthält. Man erhalte folgendes Schema

$$\begin{array}{cccccc}
\sigma_1=1, & \sigma_2, & \sigma_3, & \dots & \sigma_x; & \Gamma,\\
\mathfrak{s}_2\sigma_1, & \mathfrak{s}_2\sigma_2, & \mathfrak{s}_2\sigma_3, & \dots & \mathfrak{s}_2\sigma_x; & \mathfrak{s}_2\Gamma,\\
\dots & \dots & \dots & \dots & \dots & \dots\\
\mathfrak{s}_y\sigma_1, & \mathfrak{s}_y\sigma_2, & \mathfrak{s}_y\sigma_3, & \dots & \mathfrak{s}_y\sigma_x; & \mathfrak{s}_y\Gamma,
\end{array}$$

wobei die $\mathfrak{s}_2$, $\mathfrak{s}_3$, $\dots$ nach dem einfachen Prinzipe ausgewählt werden können, dass eine jede unter denjenigen Substitutionen von G_1 gewählt wird, welche den Komplexen Γ, bez. Γ und $\mathfrak{s}_2\Gamma$ u. s. f. noch

nicht angehörten. Die Gruppe G'_1 kann ebenso behandelt werden; sie führe auf $\mathfrak{S}'_2, \mathfrak{S}'_3, \ldots \mathfrak{S}'_{g'}$. So kann jedes

$$s_\alpha = \mathfrak{S}_\beta \sigma_\gamma, \quad \text{jedes} \quad s'_\alpha = \mathfrak{S}'_\beta \sigma_\gamma$$

gesetzt werden.

Das Produkt $s_\alpha^{-1} s'^{-1}_\beta s_\alpha s'_\beta = s_\alpha^{-1}(s'^{-1}_\beta s_\alpha s'_\beta) = (s_\alpha^{-1} s'^{-1}_\beta s_\alpha) \cdot s'_\beta$ gehört seiner zweiten Form halber zu G_1; denn wegen

$$G^{-1} G_1 G = G_1 \quad \text{ist} \quad s'^{-1}_\beta s_\alpha s'_\beta = s_\gamma,$$

und also wird das obige Produkt $= s_\alpha^{-1} s_\gamma$; es gehört der dritten Form halber zu G'_1; denn wegen

$$G^{-1} G'_1 G = G'_1 \quad \text{ist} \quad s_\alpha^{-1} s'^{-1}_\beta s_\alpha = s'_\gamma,$$

und daher wird das obige Produkt $= s'_\gamma \cdot s'_\beta$. Folglich gehört das Produkt zu der Gruppe Γ, welche G_1 und G'_1 gemeinsam haben:

A) $$s_\alpha^{-1} s'^{-1}_\beta s_\alpha s'_\beta = \sigma_\gamma; \quad s_\alpha s'_\beta = s'_\beta s_\alpha \sigma_\gamma; \quad s'_\beta s_\alpha = s_\alpha s'_\beta \sigma_\delta.$$

Insbesondere erhalten wir, da die σ zu den s und zu den s' gehören,

B) $$\sigma_\alpha \mathfrak{S}'_\beta = \mathfrak{S}'_\beta \sigma_\gamma; \quad \sigma_\alpha \mathfrak{S}_\beta = \mathfrak{S}_\beta \sigma_\delta; \quad \mathfrak{S}'_\alpha \mathfrak{S}_\beta = \mathfrak{S}_\beta \mathfrak{S}'_\alpha \sigma_\varepsilon.$$

Hieraus folgt, dass die Substitutionen der Form $\mathfrak{S}_\alpha \mathfrak{S}'_\beta \sigma_\gamma$ eine Gruppe bilden; denn man hat durch wiederholte Anwendung der Gleichungen B)

$$(\mathfrak{S}_\alpha \mathfrak{S}'_\beta \sigma_\gamma)(\mathfrak{S}_a \mathfrak{S}'_b \sigma_c) = \mathfrak{S}_\alpha \mathfrak{S}'_\beta \mathfrak{S}_a \sigma_\delta \mathfrak{S}'_b \sigma_c = \mathfrak{S}_\alpha \mathfrak{S}_a \cdot \mathfrak{S}'_\beta \sigma_\varepsilon \mathfrak{S}'_b \sigma_c = \mathfrak{S}_\alpha \mathfrak{S}_a \mathfrak{S}'_\beta \mathfrak{S}'_b \sigma_d$$
$$= \mathfrak{S}_\zeta \sigma_e \mathfrak{S}'_\eta \sigma_f \sigma_d = \mathfrak{S}_\zeta \mathfrak{S}'_\eta \sigma_\vartheta.$$

Die Gruppe $\mathfrak{G}$ der Substitutionen $\mathfrak{S}_\alpha \mathfrak{S}'_\beta \sigma_\gamma$ ist mit G vertauschbar, denn es ist

$$G^{-1}(\mathfrak{S}_\zeta \mathfrak{S}'_\eta \sigma_\vartheta) G = G^{-1} \mathfrak{S}_\zeta G \cdot G^{-1} \mathfrak{S}'_\eta \sigma_\vartheta G = s_\alpha \cdot s'_\beta = \mathfrak{S}_\gamma \sigma_\delta \cdot \mathfrak{S}'_\varepsilon \sigma_\iota = \mathfrak{S}_\gamma \mathfrak{S}'_\varepsilon \sigma_\varkappa.$$

Die Gruppe $\mathfrak{G}$ ist umfassender als G_1 und als G'_1; sie ist in G enthalten; also ist sie nach den Voraussetzungen über G_1 und G'_1 mit G identisch.

Die Ordnung von $\mathfrak{G}$ ist gleich $xy.y'$; denn es ergiebt sich aus $\mathfrak{S}_a \mathfrak{S}'_b \sigma_c = \mathfrak{S}_\alpha \mathfrak{S}'_\beta \sigma_\gamma$ leicht $a = \alpha$, $b = \beta$, $c = \gamma$. Folglich wird auch die Ordnung von G gleich xyy', und da

$$r = r_1 e_1 = xy e_1, \quad r = r'_1 e'_1 = xy' e'_1$$

ist, so folgt

$$y' = e_1, \quad y = e'_1.$$

Durch dieses letzte Resultat haben wir die Ordnung von Γ, nämlich $x = \dfrac{r}{e_1 e'_1} = \dfrac{r_1}{e'_1} = \dfrac{r'_1}{e_1}$ kennen gelernt. Es lässt sich von Γ weiter zeigen, dass diese Gruppe in eine der Reihen, die zu G_1 (und dann auch ebenso zu G'_1) gehören, einrangiert werden kann, da sie eine ausgezeichnete Maximaluntergruppe von G_1 und von G'_1 ist. Denn zuerst ist Γ, als Teil von G'_1 mit G_1, und ferner als Teil von G_1 mit G'_1 vertauschbar; man hat daher

$$G_1^{-1} \Gamma G_1 = G'_1, \quad G'^{-1}_1 \Gamma G'_1 = G_1;$$

da aber die linke Seite der ersten Gleichung völlig der Gruppe G_1 angehört, so findet dasselbe auch rechts statt; ähnlich steht es mit der zweiten Gleichung; also ist

$$G_1^{-1}\Gamma G_1 = \Gamma; \quad G'^{-1}_1 \Gamma G'_1 = \Gamma.$$

Ausserdem lässt sich zeigen, dass zwischen G_1 und Γ keine zu G_1 vertauschbare Gruppe besteht, welche Γ umfasst. Wäre eine solche H mit den Substitutionen t_α vorhanden, so wäre nach A)

$$t_\alpha^{-1} s'^{-1}_\beta t_\alpha s'_\beta = \sigma_\gamma, \quad \text{also} \quad s'^{-1}_\beta t_\alpha s'_\beta = t_\alpha \,.\, t_\alpha^{-1} s'^{-1}_\beta t_\alpha s'_\beta = t_\alpha \sigma_\gamma = t_\delta,$$

d. h. es wäre H auch mit G'_1 vertauschbar, und da G sich aus den Substitutionen von G_1 und G'_1 zusammensetzt, so wäre H auch mit G vertauschbar.

Setzt man nun die $s'_2, s'_3, \ldots$ mit den t_α zusammen, so bilden die $s'_\alpha t_\beta$ eine Gruppe; denn nach A) hat man, da Γ in H und in G_1 enthalten ist,

$$(s'_\alpha t_\beta)(s'_\gamma t_\delta) = s'_\alpha \,.\, s'_\gamma t_\beta \sigma_\varepsilon \,.\, t_\delta = s'_\alpha t_b.$$

Diese Gruppe ist mit G vertauschbar, da H und G'_1, aus denen sie sich zusammensetzt, es sind; sie enthält G'_1, welches bereits durch die Substitutionen $s'_\alpha \sigma_\beta$ gebildet wird; sie ist in G enthalten, welches aus den $s'_\alpha s_\beta \sigma_\gamma$ besteht. Daher widerspricht sie der über G'_1 gemachten Voraussetzung, dass diese Gruppe eine ausgezeichnete Maximaluntergruppe von G sei. Wir erhalten also das Zwischenresultat: Folgt in einer zu G gehörigen Reihe G_1 auf G, in einer anderen Reihe G'_1 auf G, so kann man in beiden auf G_1, respektive G'_1 eine und dieselbe ausgezeichnete Maximaluntergruppe Γ folgen lassen, welche aus allen Substitutionen besteht, die G_1 und G'_1 gemein haben. Ist dabei e_1 der zu G_1 gehörige Faktor der Zusammensetzung, e'_1 der zu G'_1 gehörige, so hat Γ in Bezug auf G_1 den Faktor e'_1, in Bezug auf G'_1 den Faktor e_1.

§ 82. Hieraus können wir leicht den zu beweisenden Satz folgern.

Eine Reihe der zu G gehörigen ausgezeichneten Maximaluntergruppen sei:

1)
$$G, G_1, G_2, G_3, \ldots,$$
$$r, \quad r_1 = \frac{r}{e_1}, \quad r_2 = \frac{r_1}{e_2}, \quad r_3 = \frac{r_2}{e_3}, \ldots;$$

eine andere der zu G gehörigen Reihen sei die nachstehende:

2)
$$G, G'_1, G'_2, G'_3, \ldots,$$
$$r, \quad r'_1 = \frac{r}{e'_1}, \quad r'_2 = \frac{r'_1}{e'_2}, \quad r'_3 = \frac{r'_2}{e'_3}, \ldots$$

Dann kann man nach dem eben bewiesenen Zwischenresultate zwei neue zu G gehörige Reihen konstruieren:

3) $G, G_1, \Gamma, \Delta, H, \ldots$ $\quad r, \; r_1 = \frac{r}{e}, \; r'_2 = \frac{r_1}{e'_1}, \cdots$

4) $G, G'_1, \Gamma, \Delta, H, \ldots$ $\quad r, \; r'_1 = \frac{r}{e'_1}, \; r'_2 = \frac{r'_1}{e}, \cdots$

und den Beweis von der Konstanz der Faktoren der Zusammensetzung bei 1) und bei 2) übertragen auf denselben Beweis bei den Reihen 1) und 3) einerseits und 2) und 4) andererseits; denn dass 3) und 4) dieselben Faktoren der Zusammensetzung liefern, zeigt der erste Blick.

Der Nachweis für 1) und 3) und für 2) und 4) reduziert aber die Schwierigkeit. Denn während 1) und 2) nur in dem ersten Gliede übereinstimmten, stimmen 1) und 3) ebenso wie 2) und 4) je in den beiden ersten Gliedern überein.

Der Fortgang des Beweises wird der sein, dass man in 1) und 3) auf die beiden ersten gemeinsamen Glieder G, G_1, denen einmal G_2 und einmal Γ folgt, zwei neue Reihen aufbaut

1') $G, G_1, G_2, \mathfrak{G}, \mathfrak{H}, \mathfrak{J}, \ldots$ $\quad r, \; r_1, \; r_2 = \frac{r_1}{e_2}, \; r''_3 = \frac{r_2}{e'_2}, \cdots$

3') $G, G_1, \Gamma, \mathfrak{G}, \mathfrak{H}, \mathfrak{J}, \ldots$ $\quad r, \; r_1, \; r'_2 = \frac{r_1}{e'_2}, \; r''_3 = \frac{r'_2}{e_2}, \cdots$

welche dieselben Kompositionsfaktoren haben, und von denen 1') mit 1) und 3') mit 3) bereits in drei Gliedern übereinstimmen, u. s. w.

So gelangt man zu dem Resultate:

Lehrsatz XVIII. Giebt es verschiedene zur zusammengesetzten Gruppe G gehörige Reihen, so stimmen die Faktoren der Zusammensetzung für diese bis auf ihre Aufeinanderfolge überein. Daher ist auch die Anzahl der Gruppen dieser Reihen konstant.

§ 83. Wir betrachten zwei aufeinanderfolgende Gruppen einer solchen Reihe, oder, was dasselbe ist, eine Gruppe G und eine ausgezeichnete Maximaluntergruppe H von G. Es sei s'_1 eine von den Substitutionen der Gruppe G, die nicht auch in H vorkommen; s'^m_1 sei die niedrigste Potenz von s'_1, welche in H bereits vorkommt. (m ist gleich der Ordnung von s'_1 oder gleich einem Teiler derselben.) Ist m eine zusammengesetzte Zahl und $= p.q$, so setzen wir $s'^q_1 = s_1$ und erhalten dadurch eine Substitution s_1, welche H nicht angehört und von der eine Primzahlpotenz s^p_1 die erste in H auftretende sein wird. Jetzt transformieren wir s_1 durch alle Substitutionen von G und erhalten dadurch $s_1, s_2, \ldots s_\lambda$. Keine von diesen kann H angehören.

Denn wäre dies bei $s_\alpha = \sigma^{-1} s_1 \sigma$ der Fall, so würde $\sigma s_\alpha \sigma^{-1} = s_1$, die Transformierte einer Substitution s_α von H durch eine Substitution σ^{-1} von G auch zu H gehören, da H mit G vertauschbar ist. Das widerspräche der Annahme. Wir betrachten jetzt

$$\Gamma = \{H; s_1, s_2, \ldots s_\lambda\}.$$

Diese Gruppe enthält H und ist in G enthalten. Bezeichnen wir durch t eine beliebige Substitution von G, so wird

$$t^{-1}\Gamma t = t^{-1}\{H . s_1^{\alpha} s_2^{\beta} \ldots\} t = t^{-1} H t . t^{-1} s_1^{\alpha} t . t^{-1} s_2^{\beta} t \ldots$$
$$= H . s_{i_1}^{\gamma} s_{i_2}^{\delta} \ldots = \Gamma;$$

es ist also Γ mit G vertauschbar. Die drei so bewiesenen Eigenschaften von Γ widersprechen der Annahme, dass H eine ausgezeichnete Maximaluntergruppe von G ist; und dieser Widerspruch lässt sich nur dadurch heben, dass man annimmt, es fiele Γ mit G zusammen.

Bedenkt man ferner, dass alle Substitutionen, die durch Transformationen aus einander entspringen, einander ähnlich sind, also hier $s_1, s_2, \ldots s_\lambda$, so erkennt man:

Lehrsatz XIX. Jede Gruppe der Reihe von G ist aus der nächstfolgenden (oder: jede Gruppe ist aus einer ihrer ausgezeichneten Maximaluntergruppen) durch Hinzufügung einer Reihe von Substitutionen ableitbar, die 1) einander ähnlich sind, und von denen 2) eine Primzahlpotenz zur Gruppe geringerer Ordnung gehört. Die letzte Gruppe der Reihe einer zusammengesetzten Gruppe G wird durch eine Anzahl einander ähnlicher Substitutionen von Primzahlordnung gebildet.

§ 84. Hierher gehört der folgende für die Theorie der Gleichungen wichtige Satz:

Lehrsatz XX. Die Reihe der Zusammensetzung, welche zur symmetrischen Gruppe von n Elementen gehört, besteht aus der alternierenden Gruppe und der Einheit, wenn $n > 4$ ist; die Faktoren der Zusammensetzung sind also 2 und $\frac{1}{2}n!$ Die alternierende Gruppe von mehr als vier Elementen ist einfach.

Dass die alternierende Gruppe mit jeder beliebigen Substitution vertauschbar und also ausgezeichnete Maximaluntergruppe der symmetrischen ist, erkennt man.

Es ist weiter nachzuweisen, dass für $n > 4$ die alternierende Gruppe einfach ist. Der Beweis gestaltet sich dem in § 50 gegebenen ganz ähnlich, wie denn auch der dortige Satz, in die jetzige Ausdrucksweise

übersetzt, dem obigen ähnlich lautet, nämlich: Eine Gruppe, welche mit der symmetrischen vertauschbar, also eine ausgezeichnete Untergruppe derselben ist, wird für $n > 4$ die alternierende werden oder sich auf die Einheit zusammenziehen. Es wird daher auch nur eine kurze Andeutung des Beweises nötig sein.

Es werde in der Gruppe H_1, die eine ausgezeichnete Maximaluntergruppe von der alternierenden Gruppe H sein soll, eine Substitution von möglichst geringer Elementenzahl betrachtet. Diese kann nicht mehr als drei Elemente in einem Cyklus haben; denn wäre

$$s = (x_1 x_2 x_3 x_4 \ldots)$$

eine solche Substitution, so transformiert man sie durch die Substitution $\sigma = (x_2 x_3 x_4)$, die ja in H vorkommt; $s^{-1} . \sigma^{-1} s \sigma$ enthält dann gegen die Voraussetzung weniger Elemente als σ. Ferner können die Substitutionen geringster Elementenzahl nur einen Cyklus haben. Denn wenn

$$s_\alpha = (x_1 x_2)(x_3 x_4) \ldots \quad \text{oder} \quad s_\beta = (x_1 x_2 x_3)(x_5 x_4 x_6) \ldots$$
$$\text{oder} \quad s_\gamma = (x_1 x_2)(x_3 x_4 x_5) \ldots$$

in H vorkäme, so transformierte man in den beiden ersten Fällen durch $\sigma = (x_1 x_2 x_5)$, im letzten durch $\tau = (x_1 x_2)(x_3 x_4)$, und es werden in den Produkten

$$s_\alpha . \sigma^{-1} s_\alpha \sigma, \quad \text{respektive} \quad s_\beta . \sigma^{-1} s_\beta \sigma, \quad s_\gamma . \tau^{-1} s_\gamma \tau$$

weniger Elemente vorkommen, als in s_α, s_β, s_γ entsprechend. Dies verletzt die Voraussetzung. Die Substitutionen geringster Elementenzahl können also nur

$$s = (x_\alpha x_\beta), \quad t = (x_\alpha x_\beta x_\gamma)$$

sein. Der erste Fall ist nicht möglich, da in der alternierenden Gruppe keine Transposition vorkommt. Der zweite Fall führt auf die alternierende Gruppe selbst zurück.

Ist $n = 4$, so erhält man folgende Reihe: 1) die symmetrische, 2) die alternierende Gruppe; 3) $G_2 = [1, (x_1 x_2)(x_3 x_4), (x_1 x_3)(x_2 x_4), (x_1 x_4)(x_2 x_3)]$; 4) $G_3 = [1, (x_1 x_2)(x_3 x_4)]$; 5) $G_4 = 1$. Der Ausnahmegruppe G_2 begegneten wir schon mehrfach.

§ 85. Von gleicher Wichtigkeit für die algebraische Auflösung von Gleichungen wie die eben besprochene Reihe der Zusammensetzung einer Gruppe G ist ihre Hauptreihe der Zusammensetzung, oder kurz ihre Hauptreihe. Wir bilden dieselbe aus der Reihe von G einfach dadurch, dass wir alle und nur diejenigen Gruppen der Reihe zurückbehalten, welche mit G selbst vertauschbar sind. So möge

$$G, H, J, \ldots K, L, M, 1$$

entstehen. Die Reihe von G kann gleichzeitig Hauptreihe sein. Dies tritt z. B., wie wir sofort nachweisen werden, dann ein, wenn alle Faktoren der Zusammensetzung von einander verschiedene Primzahlen sind.

Angenommen, die Hauptreihe von G stimmt nicht mit der Reihe von G überein, dann mögen sich in der Reihe von G, z. B. zwischen H und J noch Gruppen einschieben, etwa

$$H,\ H_1,\ H_2,\ \ldots\ H_{\nu-1},\ J,$$

derart, dass die Mittelglieder zur Reihe, aber nicht zur Hauptreihe gehören. H_1 ist demnach mit H vertauschbar, aber nicht mit G. Infolgedessen ist

$$H^{-1}H_1H = H_1, \quad G^{-1}H_1G \neq H_1.$$

Transformieren wir H_1 durch alle Substitutionen von G, so werden demnach verschiedene Gruppen H_1, H'_1, H''_1, ... entstehen. Diese sind sämtlich in H enthalten, denn es ist

$$\sigma^{-1}H_1\sigma = H'_1 \quad \text{in} \quad \sigma^{-1}H\sigma = H$$

enthalten, wenn σ eine Substitution von G bedeutet; und weiter ist

$$H^{-1}H'_1H = H^{-1}.\sigma^{-1}H_1\sigma.H = (\sigma^{-1}H^{-1}\sigma)(\sigma^{-1}H_1\sigma)(\sigma^{-1}H\sigma)$$
$$= \sigma^{-1}.H^{-1}H_1H.\sigma = \sigma^{-1}H_1\sigma = H'_1.$$

Ist nämlich τ eine Substitution von H, so wird sich aus $\sigma^{-1}\tau\sigma = v$ ergeben $\sigma^{-1}\tau^{-1}\sigma = v^{-1}$ (vergl. S. 37 § 36).

Ferner ist J in jeder Gruppe H_1, H'_1, H''_1, ... enthalten; denn es ist J in H_1 und also

$$\sigma^{-1}J\sigma = J \quad \text{in} \quad \sigma^{-1}H_1\sigma = H'_1$$

enthalten. Endlich ist H'_1 wie H_1 eine ausgezeichnete Maximaluntergruppe von H. Denn wenn eine ausgezeichnete Untergruppe H'_1 zwischen H und H'_1 bestände, dann würde auf eine gleiche zwischen H und H_1 zu schliessen sein; man würde dieselbe aus H'_1 durch Transformation mit σ^{-1} erhalten, wenn H'_1 aus H_1 durch Transformation mit σ hervorgeht.

Es folgen also in der Reihe von G auf H mehrere von einander verschiedene Gruppen H_1, H'_1, ... von gleichem Typus. Alle diese gehören demnach zu demselben Faktor ε der Zusammensetzung; dies ist der Quotient der Ordnungen von H und von H_1. Dann können wir nach dem Zwischenresultate in § 81 die Reihe von G derart fortsetzen, dass wir die gemeinsamen Substitutionen z. B. von H_1 und von H'_1, von H_1 und von H''_1, von H_1 und von H'''_1, ... auf H_1 folgen lassen. Nach demselben Resultate gehören die neuen Gruppen wiederum zum Faktor ε. Jede von ihnen enthält J. Wir brauchen natürlich nur die von einander verschiedenen so entstehenden Gruppen

beizubehalten. Giebt es nur eine derselben, so stimmt diese mit J überein. Denn die Gesamtheit der Gruppe

$$H_1, H'_1, H''_1, H'''_1, \ldots$$

und daher auch die ihnen allen gemeinsame Gruppe ändert sich bei Transformationen durch Substitutionen von G nicht. Die Ordnung von J wird dann aus der von H durch Division mit ε^2 erhalten.

Sind dagegen noch mehrere verschiedene Gruppen vorhanden, so kann man in derselben Weise weitergehen. Die gemeinsamen Substitutionen z. B. von H_1, H'_1, H''_1 bilden eine Gruppe, welche in der Reihe von G auf die Gruppe folgen kann, in der alle gemeinsamen Substitutionen von H_1, H'_1 vorkommen. Der zugehörige Faktor der Zusammensetzung ist wieder ε.

Nach ν Schritten langt man bei J an; die Ordnung von J entsteht also durch Division mit ε^ν aus der von H. Die letzte Stufe von J bilden ν Gruppen $H_{\nu-1}, H'_{\nu-1}, \ldots$ welche einander sämtlich ähnlich sind, zum Faktor ε gehören und

$$H = \{H_{\nu-1}, H'_{\nu-1}, H''_{\nu-1}, \ldots\}$$

liefern.

Lehrsatz XXI. Stimmt die Hauptreihe von G nicht mit der Reihe der Zusammensetzung überein, sondern schieben sich zwischen zwei Gruppen H, J der ersteren $\nu - 1$ Gruppen $H_1, H_2, \ldots H_{\nu-1}$ der letzteren ein, so gehören zu $H_1, H_2, \ldots J$ gleiche Faktoren der Zusammensetzung ε und die Ordnung r' von H entsteht aus der Ordnung r'' von J durch Multiplikation mit ε^ν. H kann aus J erhalten werden, indem man mit J eine Reihe von ν Gruppen $H_{\nu-1}, H'_{\nu-1}, \ldots$ vereinigt, die einander ähnlich und von der Ordnung $r''.\varepsilon$ sind.

Zusatz I. Eine Gruppe, deren Faktoren der Zusammensetzung einander nicht sämtlich gleich sind, besitzt eine Hauptreihe.

Zusatz II. Jede imprimitive Gruppe ist zusammengesetzt. Enthält dieselbe umfassendere und engere Systeme der Imprimitivität, so besitzt sie eine Hauptreihe.

Zusatz III. Die Gruppen $H_{\nu-1}, H'_{\nu-1}, H''_{\nu-1}, \ldots$ sind miteinander vertauschbar, d. h. es gelten die Gleichungen

$$H_{\nu-1}{}^{(\alpha)} H_{\nu-1}{}^{(\beta)} = H_{\nu-1}{}^{(\beta)} H_{\nu-1}{}^{(\alpha)}.$$

Denn man kann in der Reihe vor J die Gruppenfolge $H_{\nu-1}{}^{(\alpha)}$, $\{H_{\nu-1}{}^{(\alpha)}, H_{\nu-1}{}^{(\beta)}\}$, ... annehmen. Also ist

$$(H_{\nu-1}{}^{(\alpha)} H_{\nu-1}{}^{(\beta)})^{-1} H_{\nu-1}{}^{(\alpha)} (H_{\nu-1}{}^{(\alpha)} H_{\nu-1}{}^{(\beta)}) = H_{\nu-1}{}^{(\alpha)}.$$

Zusatz IV. Die letzte Gruppe M der Hauptreihe von G besteht aus einer oder aus mehreren einander ähnlichen Gruppen, welche ausser der Einheit keine Substitutionen miteinander gemeinsam haben, und welche miteinander vertauschbar sind.

§ 86. Es ist der wichtige Spezialfall zu betrachten, dass ε eine Primzahl $= p$ wird.

Statt der $H'_{\nu-1}, H''_{\nu-1}, \ldots$ führen wir die bequemeren Bezeichnungen

$$H', H'', H''', \ldots H^{(\nu)}$$

ein. Dann entsteht H' aus J durch Hinzunahme einer Substitution t_1, bei welcher die p^{te} Potenz die erste in J vorkommende ist. Wir können setzen (§ 83)

$$H' = t_1^{\alpha} J, \quad H'' = t_2^{\alpha} J, \quad H''' = t_3^{\alpha} J, \ldots \quad (\alpha = 0, 1, \ldots p-1)$$

Da J eine ausgezeichnete Untergruppe jeder der Gruppen H', H'', ... ist, so wird

$$t_1^{-\alpha} J t_1^{\alpha} = J, \quad t_2^{-\alpha} J t_2^{\alpha} = J, \quad t_3^{-\alpha} J t_3^{\alpha} = J, \ldots$$

und wenn wir die Substitutionen von J mit $i_1, i_2, i_3, \ldots$ bezeichnen

$$t_1^{-\alpha} i_1^{-1} t_1^{\alpha} = i_2, \qquad t_2^{-\alpha} i_1 t_2^{\alpha} = i_3, \qquad t_3^{-\alpha} i_1 t_3^{\alpha} = i_4, \ldots$$
$$t_1^{\alpha} i_1 = i_1 t_1^{\alpha} . (i_2 i_1), \quad t_2^{\alpha} i_1 = i_1 t_2^{\alpha} (i_3 i_1), \quad t_3^{\alpha} i_1 = i_1 t_3^{\alpha} (i_4 i_1), \ldots$$

d. h. es sind die Substitutionen von H', ebenso die von H'', die von H''' u. s. w. unter sich bis auf Substitutionen von J vertauschbar.

Da man, um von J rückwärts zu H zu gelangen, die Substitutionen z. B. von H' und von H'' in eine Gruppe vereinigen kann (§ 81), so ist (§ 85, Zusatz III)

$$t_2^{-1} t_1 t_2 = t_1^{\alpha} i_1, \quad t_1^{-1} t_2^{-1} t_1 = t_2^{\beta} i_2,$$

folglich durch Kombination beider Resultate

$$t_1^{-1} t_2^{-1} t_1 t_2 = t_2^{\beta} i_2 t_2 \quad = t_2^{\beta+1} i_3,$$
$$= t_1^{-1} t_1^{\alpha} i_1 = t_1^{\alpha-1} i_1,$$
$$t_1^{\alpha-1} i_1 = t_2^{\beta+1} i_3.$$

Die linke Seite dieser Gleichung ist eine Substitution aus H', die rechte ist eine solche aus H''. Da beide Gruppen nur die Substitutionen von J gemeinsam haben, müssen die Potenzen von t_1 und von t_2 verschwinden, d. h. es muss sein $\alpha = 1$, $\beta = -1$ und

$$t_2^{-1} t_1 t_2 = t_1 i_1,$$
$$t_1 t_2 = t_2 t_1 i_1,$$
$$(t_1 i_1)(t_2 i_2) = (t_2 i_2)(t_1 i_1) . i_3,$$
$$(t_1^{\alpha} i_1)(t_2^{\beta} i_2) = (t_2^{\beta} i_2)(t_1^{\alpha} i_1) . i_4.$$

Also sind die Substitutionen der aus J, t_1, t_2 gebildeten Gruppe untereinander bis auf Substitutionen von J vertauschbar. Dasselbe folgt für die aus J, t_1, t_3 und für die aus J, t_2, t_3 gebildete Gruppe, also auch für die Gruppe $\{J, t_1, t_2, t_3\}$ u. s. w, also schliesslich auch für H selbst. (Zu bemerken ist, dass § 85 Zusatz III) bei weitem weniger aussagt; denn dort handelt es sich um Vertauschbarkeit von Gruppen, hier um die Vertauschbarkeit der einzelnen Substitutionen.) Je zwei Substitutionen von H sind untereinander bis auf eine Substitution von J vertauschbar, welche als Faktor dazutritt.

Wir werden die Umkehrung dieses Satzes beweisen: Sind je zwei Substitutionen von H bis auf eine Substitution von J gegen einander vertauschbar, so ist ε eine Primzahl. Ja, dies findet sogar schon statt, wenn die Substitutionen von H' untereinander bis auf solche von J vertauschbar sind. Steht dies nämlich fest und wäre gleichzeitig ε eine zusammengesetzte Zahl, so mögen q, q', q'', ... ihre Primfaktoren sein. Wir wählen aus H'_1 eine Substitution t aus, die nicht schon in J vorkommt und gemäss § 83 Lehrsatz XIX) gewählt ist. Dann wird z. B. t^q die niedrigste Potenz von t sein, welche in J auftritt.

Transformieren wir nun

$$H'^{-1}.(t^\alpha J)\,H' = H'^{-1}t^\alpha H'.H'^{-1}JH'$$
$$= H'^{-1}t^\alpha H'J,$$

so wird der Voraussetzung nach $t^\alpha H' = H't^\alpha J$ sein, also

$$H'^{-1}(t^\alpha J)\,H' = t^\alpha J$$

werden. Die Gruppe $\{t, J\}$ ist also eine ausgezeichnete Untergruppe von H', welche J enthält und umfassender ist als J. Sie ist ferner in H' enthalten und weniger umfassend als diese Gruppe. Denn, weil t mit J vertauschbar ist, hat man nach §§ 37, 38 die Ordnung von $\{t, J\}$ gleich $r''.q < r''\varepsilon$ zu setzen. Dies geht gegen unsere Annahme, dass J in der Reihe von G unmittelbar auf H' folgen solle.

Lehrsatz XXII. Wenn in der Hauptreihe der Zusammensetzung von G die Ordnung r' von H aus der Ordnung r'' von J durch Multiplikation mit p^ν abgeleitet werden kann, wobei die Primzahl p der Faktor der Zusammensetzung für die Gruppen der zugehörigen Zwischenglieder ist, dann sind die Substitutionen von H bis auf solche von J gegen einander vertauschbar; und wenn dies eintritt, dann sind umgekehrt alle Faktoren der Zusammensetzung für die Gruppen zwischen H und J gleich einer Primzahl p.

§ 87. Wir betrachten zwei Gruppen G und Γ; jeder Substitution von G mögen eine oder mehrere Substitutionen von Γ zugeordnet werden können und umgekehrt jeder von Γ eine einzige von G derart, dass jedem Produkte zweier Substitutionen der einen das Produkt der entsprechenden Substitutionen der anderen Gruppe zugeordnet erscheint. Ist je einer Substitution von G nur eine von Γ zugeordnet, so nennen wir diese Beziehung einstufigen Isomorphismus, sind einer Substitution von G mehrere von Γ zugeordnet, mehrstufigen Isomorphismus.*

Beispiele. Ist

$$G = [1,\ (x_1 x_2)],$$
$$\Gamma = [1,\ (\xi_1\xi_2)(\xi_3\xi_4);\ \ (\xi_1\xi_3)(\xi_2\xi_4),\ \ (\xi_1\xi_4)(\xi_2\xi_3)],$$

so ist G zweistufig isomorph zu Γ derart, dass die beiden ersten Substitutionen von Γ der Substitution 1 von G, die beiden letzten von Γ der Substitution $(x_1 x_2)$ von G entsprechen.

Ist

$$G = [1,\ (x_1x_2)(x_3x_6)(x_4x_5),\ (x_1x_3)(x_2x_5)(x_4x_6),\ (x_1x_4)(x_2x_6)(x_3x_5),$$
$$(x_1x_5x_6)(x_2x_3x_4),\ (x_1x_6x_5)(x_2x_4x_3)],$$
$$\Gamma = [1,\ (\xi_1\xi_2),\ (\xi_1\xi_3),\ (\xi_2\xi_3),\ (\xi_1\xi_2\xi_3),\ (\xi_1\xi_3\xi_2)],$$

so findet zwischen G und Γ einstufiger Isomorphismus statt; man kann jede Substitution von G der an entsprechender Stelle bei Γ stehenden zuordnen. Multipliziert man zwei Substitutionen von G und die entsprechenden von Γ, so entsprechen sich auch beide Produkte.

§ 88. Sind G und Γ einstufig isomorph, so haben sie gleiche Ordnungen.

Ist G zu Γ mehrstufig isomorph, und entspricht der Substitution 1 von G eine Reihe von Substitutionen $\sigma_1, \sigma_2, \sigma_3, \ldots \sigma_m$ von Γ, so bilden die letzteren eine Untergruppe von Γ. Denn $\sigma_\alpha . \sigma_\beta$ entspricht dem Produkte $1.1 = 1$ und findet sich also wieder unter den σ. Diese Gruppe

$$\Sigma = [\sigma_1 = 1,\ \sigma_2 \ldots \sigma_m]$$

ist eine ausgezeichnete Untergruppe zu Γ. Denn bedeutet τ eine beliebige Substitution von Γ, welcher t aus G entspricht, so entsprechen sich die beiden Produkte

$$\tau^{-1}\sigma_\alpha\tau \quad \text{und} \quad t^{-1}.1.t = 1,$$

folglich gehört $\tau^{-1}\sigma_\alpha\tau$ wieder zu Σ.

---

* C. Jordan: Traité etc. §§ 67–74. Dort sind die Namen „holoedrischer" und „meriedrischer Isomorphismus" eingeführt, wo wir die Bezeichnung „einstufig", „mehrstufig" gebrauchen.

Ist τ_2 eine Substitution von Γ, welche irgend einer von der Einheit verschiedenen Substitution s_2 von G entspricht, dann bilden wir eine Tabelle, deren erste Zeile Σ, deren zweite

$$\sigma_1\tau_2,\ \sigma_2\tau_2,\ \sigma_3\tau_2,\ \ldots\ \sigma_m\tau_2;\quad \Sigma\tau_2$$

sein mag. Wir können dann wie gewöhnlich beweisen: 1) dass alle die Substitutionen der zweiten Zeile und 2) auch nur sie der Substitution s_2 entsprechen; 3) dass sie untereinander und 4) von denen der ersten Zeile verschieden sind. Ist dann s_3 eine dritte Substitution von G, dann lässt sich die Anordnung fortsetzen und man erkennt: Ist G mehrstufig isomorph zu Γ, so gehören zu jeder Substitution von G gleichviele Substitutionen von Γ; die Ordnung von Γ ist m mal grösser als die von G, wenn m den Index der Mehrstufigkeit oder auch die Ordnung derjenigen Untergruppe von Γ bedeutet, die der Substitution 1 von G entspricht.

Ist L eine ausgezeichnete Untergruppe von G, Λ die entsprechende Gruppe von Γ, so ist auch Λ eine ausgezeichnete Untergruppe von Γ. Denn aus

$$G^{-1}LG = L \quad \text{folgt} \quad \Gamma^{-1}\Lambda\Gamma = \Lambda.$$

Dasselbe gilt umgekehrt.

Ist L eine ausgezeichnete Maximaluntergruppe von G, Λ die entsprechende Gruppe von Γ, so ist auch Λ eine ausgezeichnete Maximaluntergruppe von Γ. Denn gäbe es eine Gruppe Θ, welche in Γ enthalten und mit Γ vertauschbar ist, und in der Λ enthalten ist, so wird die entsprechende Gruppe T die entsprechenden Eigenschaften bei G und L besitzen, so dass L keine ausgezeichnete Maximaluntergruppe sein könnte.

Der Reihe der Zusammensetzung von G entspricht die von Γ; alle Faktoren der Zusammensetzung von G treten auch bei Γ auf. Ist G mehrstufig isomorph zu Γ, so treten in der Reihe der letzteren Gruppe noch die zur Reihe von Σ gehörigen Untergruppen und die zugehörigen Faktoren der Zusammensetzung auf. Der Beweis ist auch hier wieder leicht ersichtlich.

Ist G zu Γ mehrstufig isomorph, so ist Γ zusammengesetzt; Σ ist eine Gruppe in der Reihe der Zusammensetzung von Γ.

§ 89. Es möge G eine beliebige transitive Substitutionengruppe sein, die aus den n Elementen $x_1, x_2, \ldots x_n$ gebildet ist und die Ordnung r besitzt. Wir konstruieren eine willkürliche $n!$-wertige Funk-

tion ξ von $x_1, x_2, \ldots x_n$ mit den Werten $\xi_1, \xi_2, \ldots \xi_{n!}$ und wenden auf einen beliebigen unter ihnen ξ_1 alle r Substitutionen der Gruppe G an. Es mögen aus ξ_1 dadurch

$$\xi_1, \xi_2, \xi_3, \ldots \xi_r$$

entstehen. Dann wird der Komplex dieser Werte durch Substitutionen von G nicht geändert, da diese lediglich seine Individuen unter einander vertauschen. Die r Substitutionen von G rufen also r verschiedene Anordnungen hervor, welche wir als Substitutionen ansehen können, die unter den $\xi_1, \xi_2, \ldots \xi_r$ durchgeführt sind. Diese Substitutionen der ξ bilden, wie leicht zu sehen ist, eine Gruppe Γ. Diese Gruppe Γ ist transitiv; denn in G giebt es Substitutionen, welche ξ_1 in jeden der r Werte $\xi_1, \ldots \xi_r$ umwandeln, also giebt es in Γ Substitutionen, welche auf ξ_1 jedes der r Elemente $\xi_1, \ldots \xi_r$ folgen lassen. Jede Substitution von G wandelt alle Werte $\xi_1, \ldots \xi_r$ um, denn ξ ist eine $n!$ wertige Funktion; daher setzt jede Substitution von Γ alle r Elemente um. Die Ordnung von Γ ist gleich dem Grade dieser Gruppe, nämlich gleich r.

G und Γ sind einstufig isomorph. Denn jeder Substitution von G entspricht eine solche von Γ; umgekehrt jeder von Γ mindestens eine von G; da aber die Ordnungen beider Gruppen einander gleich sind, so entspricht auch nur eine Substitution von G einer solchen von Γ.

Lehrsatz XXIV. Zu jeder transitiven Gruppe der Ordnung r giebt es eine einstufig isomorphe transitive Gruppe, bei der Grad- und Ordnungszahl einander gleich und zwar gleich r sind.

§ 90. Lehrsatz XXV. Transitive Gruppen, deren Ordnungs- ihrer Gradzahl gleich ist, haben (mit Ausnahme der Einheit) nur Substitutionen, welche alle Elemente umsetzen. Es giebt in ihnen eine einzige Substitution, welche ein gegebenes Element auf ein vorgeschriebenes anderes folgen lässt. Jede ihrer Substitutionen besteht aus Cyklen von gleicher Ordnung. Sind zwei derartige Gruppen desselben Grades einander isomorph, was nur einstufig geschehen kann, so sind sie einander ähnlich, d. h. sie stimmen bis auf die Benennung der Elemente überein.

Die erste Reihe der Behauptungen ist grossenteils im vorigen Paragraphen bewiesen worden. Die übrigen ergeben sich fast von selbst, so dass wir nur bei der letzten Behauptung zu verweilen brauchen.

Gesetzt, Γ mit den Elementen $\xi_1, \xi_2, \ldots \xi_n$ und den Substitutionen $\sigma_1, \sigma_2, \ldots \sigma_n$ wäre isomorph zu G mit den Elementen $x_1, x_2, \ldots x_n$ und den Substitutionen $s_1, s_2, \ldots s_n$, derart, dass σ_λ und s_λ einander entsprechen. Dann ordnen wir die Elemente x_α und ξ_β einander folgendermassen zu. Zwei beliebige unter ihnen x_1, ξ_1 sollen einander entsprechen; x_1 werde durch s_λ in x_λ, ξ_1 durch das entsprechende σ_λ in ξ_λ übergeführt. Dann sollen sich auch x_λ, ξ_λ entsprechen. Da es nur je eine und stets eine Substitution giebt, welche x_1 in ein beliebiges Element x_α umwandelt, so entsteht hierbei kein Widerspruch. Jetzt muss noch bewiesen werden, dass, wenn s_λ die Folge $x_m x_n$ enthält, dann in σ_λ die Folge $\xi_m \xi_n$ vorkommt.

Es ist

$$s_m = \ldots x_1 x_m \ldots, \quad s_n = \ldots x_1 x_n \ldots; \quad s_m^{-1} s_n = \ldots x_m x_n \ldots,$$
$$\sigma_m = \ldots \xi_1 \xi_m \ldots, \quad \sigma_n = \ldots \xi_1 \xi_n \ldots; \quad \sigma_m^{-1} \sigma_n = \ldots \xi_m \xi_n \ldots$$

Da es nur eine Substitution giebt, welche auf x_m folgen lässt x_n, so ist

$$s_m^{-1} s_n = s_\lambda, \quad \sigma_m^{-1} \sigma_n = \sigma_\lambda.$$

Enthält daher s_λ einen Cyklus aus einer gewissen Anzahl von Elementen, so enthält σ_λ einen gleichen aus den entsprechenden Elementen gebildeten; daher sind erstens s_λ und σ_λ dann G und Γ von gleichem Typus.

§ 91. Sind die beiden Gruppen G, Γ einander isomorph, und ist G intransitiv, dann können wir in jeder Substitution von G alle Elemente unterdrücken, welche mit einem bestimmten unter ihnen, z. B. mit x_1 nicht in Verbindung stehen. Die zurückbleibenden Teile der einzelnen Substitutionen bilden eine neue transitive, zu Γ isomorphe Gruppe G_1, bei der aber jetzt die Mehrstufigkeit sich vervielfacht haben kann. Ist x_2 ein neues, nicht mit x_1 in transitiver Verbindung stehendes Element, dann leiten wir eine neue transitive, zu Γ isomorphe Gruppe G_2 ab, welche x_2 enthält u. s. f., bis alle Elemente untergebracht sind.

Es kann also G in eine Anzahl transitiver zu Γ isomorpher Gruppen zerlegt werden, und umgekehrt muss sich jede intransitive Gruppe aus solchen transitiven Gruppen G_1, G_2, ... zusammensetzen lassen. Bei einstufigen Isomorphismus genügt dazu die direkte Multiplikation entsprechender Bestandteile.

§ 92. Es sei G eine transitive Gruppe des Grades m und der Ordnung $r = m \cdot m_1$, welche zu Γ in k-stufigem Isomorphismus steht. Die Elemente von G seien $x_1, x_2, \ldots x_m$; G_1 möge diejenige Untergruppe von G sein, welche x_1 nicht umsetzt; ihre Ordnung ist $= m_1$. Sind

dann $s_2, s_3, \ldots$ Substitutionen von G, welche x_1 in $x_2, x_3 \ldots$ überführen, so enthalten $G_1 . s_2$, $G_1 . s_3$, ... alle Substitutionen derselben Eigenschaften und nur solche.

Dem G_1 in G entspreche Γ_1 in Γ; seine Ordnung ist $m_1 k$. Die Ordnung von Γ ist $r.k$. Wenn also φ_1 zu Γ_1 gehört, so hat φ_1 genau $\frac{rk}{m_1 k} = m$ Werte bei Anwendung aller Substitutionen von Γ. φ_2 sei derjenige, welcher aus φ_1 durch Anwendung von σ_2 entsteht, wenn σ_2 eine dem s_2 entsprechende Substitution ist. Dann enthält $\Gamma_1 . \sigma_2$ alle Substitutionen, die φ_1 in φ_2 überführen. Ähnlich sei es mit σ_3 und φ_3, σ_4 und φ_4 u. s. w., σ_m und φ_m. Wendet man alle Substitutionen von Γ auf den Komplex der Werte

$$\varphi_1, \varphi_2, \varphi_3, \ldots \varphi_m$$

an, so erhält man Komplexe, die als Substitutionen unter den m Elementen φ gedeutet werden können. Die Ordnung dieser Gruppe H ist gleich dem Quotienten von $k.r$ und der Anzahl der Substitutionen, welche alle φ ungeändert lassen. Diese entsprechen den Substitutionen, die alle x ungeändert lassen, d. h. der Substitution 1. Es giebt k diesen entsprechende in Γ; also ist die Ordnung von H gleich r. G und H haben gleichen Grad m, gleiche Ordnung r und sie sind einander isomorph, ja sogar einander ähnlich.

Denn es sei s eine Substitution von G, welche x_β auf x_α folgen lässt. Dann gehört s zu dem Komplex $s_\alpha^{-1} G_1 s_\beta$. Die entsprechende Substitution von H wird durch die Anwendung einer Substitution $\sigma_\alpha^{-1} \Gamma_1 \sigma_\beta$ auf $\varphi_1, \varphi_2, \ldots \varphi_m$ gefunden; jede dieser Substitutionen setzt φ_α in φ_β um, also unterscheidet sich die Substitution von H nur dadurch von der aus G, dass der Buchstabe x durch φ ersetzt ist.

Man kann somit alle zu Γ isomorphen Gruppen G (oder H) finden, indem man auf eine Funktion φ, welche zu einer beliebigen Untergruppe von Γ gehört, alle Substitutionen von Γ anwendet und von den Komplexen $\varphi_1, \varphi_2, \ldots \varphi_m$ zu einer Gruppe unter den Elementen φ übergeht.

Ist die gewählte Untergruppe Γ_1 eine ausgezeichnete, so wird die entstehende isomorphe Gruppe H in der Grad- und Ordnungszahl übereinstimmen, wie leicht zu sehen ist.

§ 93. Wir können den Begriff des Isomorphismus noch in der Weise erweitern,* dass wir jeder Substitution einer der beiden gegebenen Gruppen eine Anzahl von Substitutionen der anderen Gruppe zuordnen,

* A. Capelli: Battaglini G. 1878, S. 32 figg.

so dass, genau wie bisher, dem Produkte zweier Substitutionen der einen von beiden Gruppen wiederum das Produkt zweier beliebiger zugeordneter Substitutionen der anderen Gruppe zugeordnet ist.

Wir werden auf die Theorie, welche sich hieran knüpft, nicht eingehen, ihre Wichtigkeit aber daran zeigen, dass wir die Konstruktion intransitiver Gruppen aus transitiven auf diejenige von solchen gegenseitig-mehrstufig-isomorphen Gruppen zurückführen.

Lehrsatz XXVI. Multipliziert man die Substitutionen mehrerer gegenseitig-mehrstufig-isomorpher transitiver Gruppen, bei denen die Elemente einer jeden von denen jeder anderen verschieden sind, derart, dass man jede Substitution der ersten Gruppe mit je einer der zugeordneten Substitutionen jeder anderen Gruppe auf alle möglichen Weisen kombiniert und jedesmal das Produkt bildet, so entsteht eine intransitive Gruppe; und jede intransitive Gruppe kann auf die angegebene Art hergestellt werden.

Der erste Teil dieses Theorems ist leicht ersichtlich. Den zweiten beweisen wir für eine intransitive Gruppe, deren Elemente in zwei transitive Teile zerfallen. Der allgemeine Satz wird ganz ähnlich bewiesen.

Es seien die Substitutionen s_λ der intransitiven Gruppe G in die beiden Teile

$$s_\lambda = \sigma_\lambda . \tau_\lambda$$

zerlegt, wo σ_λ nur die Elemente $x_1, x_2, \ldots x_m$; τ_λ nur die Elemente $\xi_1, \xi_2, \ldots \xi_\mu$ umsetzen soll. Möglicherweise kommt σ_λ noch in anderen Verbindungen vor

$$\sigma_\lambda\tau_\lambda, \quad \sigma_\lambda\tau'_\lambda, \quad \sigma_\lambda\tau''_\lambda, \ldots$$

und ebenso τ_λ in den Verbindungen

$$\sigma_\lambda\tau_\lambda, \quad \sigma'_\lambda\tau_\lambda, \quad \sigma''_\lambda\tau_\lambda, \ldots$$

Nun ordnen wir dem σ_λ alle $\tau_\lambda, \tau'_\lambda, \tau''_\lambda, \ldots$ zu und dem τ_λ alle $\sigma_\lambda, \sigma'_\lambda, \sigma''_\lambda, \ldots$ und verfahren so mit allen Substitutionen s_λ der intransitiven Gruppe. Es bilden die σ_λ eine Gruppe Σ und die τ_λ eine Gruppe T. Der Isomorphismus beider ist zu beweisen. Es seien σ_λ, σ_μ zugeordnet den τ_λ, τ_μ; dann giebt es Substitutionen s_λ, s_μ, s_ν, so dass

$$s_\lambda = \sigma_\lambda\tau_\lambda, \quad s_\mu = \sigma_\mu\tau_\mu,$$
$$s_\lambda s_\mu = s_\nu = \sigma_\nu\tau_\nu$$

wird, und es folgt, dass $\sigma_\lambda\sigma_\mu = \sigma_\nu$ dem $\tau_\lambda\tau_\mu = \tau_\nu$ zugeordnet ist.

Fünftes Kapitel.

Algebraische Beziehungen zwischen Funktionen derselben Gruppe. Gattungen mehrwertiger Funktionen.

§ 94. Es wurde früher bewiesen, dass jeder mehrwertigen Funktion eine einzige Substitutionengruppe zugehört, derart, dass der Wert der Funktion für alle Substitutionen der Gruppe und nur für sie ungeändert bleibt. Umgekehrt sahen wir, dass zu jeder Gruppe eine unendliche Anzahl zugehöriger Funktionen gebildet werden kann. Es fragt sich, ob diese Zugehörigkeit zu einer und derselben Gruppe zu den wichtigeren Beziehungen von Funktionen unter einander gehört; speziell, ob sich aus ihr algebraische Eigenschaften folgern lassen.

Indem wir im dritten Kapitel eine Eigenschaft der Diskriminante Δ_φ von φ aus der blossen Betrachtung der Gruppe dieser Funktion herleiteten, sind wir bereits zu einer gemeinsamen algebraischen Eigentümlichkeit aller zu einer Gruppe gehörigen Funktionen gekommen, nämlich zu der, dass die Diskriminante einer solchen Funktion durch eine gewisse Potenz der Diskriminante der Grundgleichung, respektive der zu Grunde liegenden Elemente x_i teilbar sei.

§ 95. Wir werden noch eine gemeinsame Beziehung nachweisen:

Lehrsatz I. Zwei zu derselben Gruppe gehörige Funktionen sind rational durch einander darstellbar.

Es mögen φ_1 und ψ_1 zwei zur selben Gruppe G gehörige Funktionen sein. G habe die Ordnung r und den Grad n. Ist σ_2 eine nicht zu G gehörige Substitution, und sind φ_2, ψ_2 diejenigen neuen Werte, welche aus φ_1, ψ_1 vermöge der Anwendung von σ_2 hervorgehen, so findet, wenn

$$G = [s_1 = 1, s_2, s_3, \ldots s_r]$$

ist, derselbe Übergang von φ_1, ψ_1 zu φ_2, ψ_2 für alle Substitutionen

$$\sigma_2,\ s_2\sigma_2,\ s_3\sigma_2,\ \ldots\ s_r\sigma_2$$

und auch nur für sie statt. Die zu φ_2, ψ_2 gehörige Gruppe ist $\sigma_2^{-1} G \sigma_2$, die Transformierte von G durch σ_2; die neuen Werte φ_2, ψ_2 gehören wiederum zu einer und derselben Gruppe. Ist $\varrho = \frac{n!}{r} > 2$, so giebt es ausser den $2r$ Substitutionen der Formen s_α und $\sigma_2 s_\alpha$ mindestens noch eine neue Substitution σ_3, deren Anwendung von φ_1, ψ_1 die neuen Werte φ_3, ψ_3 hervorruft u. s. w., bis alle ϱ Werte von φ, ψ erhalten sind.

Es ist demnach für jedes ganzzahlige λ

$$\varphi_1{}^\lambda\psi_1 + \varphi_2{}^\lambda\psi_2 + \ldots + \varphi_\varrho{}^\lambda\psi_\varrho = A_\lambda$$

eine ganze symmetrische Funktion der Elemente $x_1, x_2, \ldots x_n$, genau wie $\varphi_1 + \varphi_2 + \ldots + \varphi_\varrho$ oder $\psi_1 + \psi_2 + \ldots + \psi_\varrho$ es waren; denn dieses Aggregat ist ja nur die Summe aller Werte, welche $\varphi_1{}^\lambda\psi_1$ annehmen kann, und daher geht dasselbe unter dem Einflusse einer beliebigen Substitution τ lediglich unter Veränderung der Stellung der einzelnen Summanden in sich selbst über. A_λ ist also auch eine rationale ganze Funktion der $c_1, c_2, \ldots c_n$, wenn φ_1, ψ_1 rationale ganze Funktionen der x_α sind.

Wir stellen nun für $\lambda = 0, 1, 2, \ldots \varrho - 1$ das System auf:

$$S) \qquad \begin{array}{llll} \psi_1 + & \psi_2 + & \psi_3 + \ldots + & \psi_\varrho = A_0, \\ \varphi_1\psi_1 + & \varphi_2\psi_2 + & \varphi_3\psi_3 + \ldots + & \varphi_\varrho\psi_\varrho = A_1, \\ \varphi_1{}^2\psi_1 + & \varphi_2{}^2\psi_2 + & \varphi_3{}^2\psi_3 + \ldots + & \varphi_\varrho{}^2\psi_\varrho = A_2, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & & & \\ \varphi_1{}^{\varrho-1}\psi_1 + & \varphi_2{}^{\varrho-1}\psi_2 + & \varphi_3{}^{\varrho-1}\psi_3 + \ldots + & \varphi_\varrho{}^{\varrho-1}\psi_\varrho = A_{\varrho-1}. \end{array}$$

Lösen wir dieses System nach den ϱ Grössen $\psi_1, \psi_2, \ldots \psi_\varrho$ auf, so erhalten wir ψ_α ausgedrückt durch $\varphi_1, \varphi_2, \ldots \varphi_\varrho$. Hierbei treten beachtenswerte Umstände ein. Es wird

$$\psi_1 = \begin{vmatrix} A_0, & 1, & 1, & \ldots 1 \\ A_1, & \varphi_2, & \varphi_3, & \ldots \varphi_\varrho \\ \vdots & \vdots & \vdots & \vdots \\ A_{\varrho-1}, & \varphi_2{}^{\varrho-1}, & \varphi_3{}^{\varrho-1}, & \ldots \varphi_\varrho{}^{\varrho-1} \end{vmatrix} : \begin{vmatrix} 1, & 1, & 1, & \ldots 1 \\ \varphi_1, & \varphi_2, & \varphi_3, & \ldots \varphi_\varrho \\ \vdots & \vdots & \vdots & \vdots \\ \varphi_1{}^{\varrho-1}, & \varphi_2{}^{\varrho-1}, & \varphi_3{}^{\varrho-1}, & \ldots \varphi_\varrho{}^{\varrho-1} \end{vmatrix} .$$

Aus bekannten Determinanteneigenschaften folgt, dass Zähler wie Nenner der rechten Seite bei der Vertauschung zweier Werte der Reihe $\varphi_2, \varphi_3, \ldots \varphi_\varrho$ untereinander lediglich ihr Zeichen ändern. Erweitert man daher mit dem Nenner und bedenkt, dass das Quadrat desselben Δ_φ wird, so erhält man

$$\psi_1 = G(A; \varphi_1; \varphi_2, \ldots \varphi_\varrho) : \Delta_\varphi,$$

wo G bei beliebiger Vertauschung zweier Werte der Reihe $\varphi_2, \varphi_3, \ldots \varphi_\varrho$ ungeändert bleibt und daher symmetrisch in $\varphi_2, \varphi_3, \ldots \varphi_\varrho$ ist. Nach dem ersten Kapitel § 8 und nach § 4 wird daher

$$\psi_1 = (a_0\varphi_1{}^{\varrho-1} + a_1\varphi_1{}^{\varrho-2} + a_2\varphi_1{}^{\varrho-3} + \ldots + a_{\varrho-1}) : \Delta_\varphi,$$

wobei die $a_0, a_1, \ldots a_{\varrho-1}$ ganze rationale Funktionen der elementaren symmetrischen Funktionen $c_1, c_2, \ldots c_n$ von $x_1, x_2, \ldots x_n$ bedeuten.

Zu denselben Resultaten gelangen wir auch auf folgende andere Art.*

* Vergl. auch den Beweis: L. Kronecker; Crelle 91, S. 307.

§ 96. Wir multiplizieren die Gleichungen des Systemes S der Reihe nach mit den noch unbestimmten Grössen $y_0, y_1, y_2, \ldots y_{\varrho-2}$ und die letzte mit $y_{\varrho-1}=1$, addieren die Produkte und setzen der Abkürzung halber

$$y_{\varrho-1}\varphi^{\varrho-1}+y_{\varrho-2}\varphi^{\varrho-2}+y_{\varrho-3}\varphi^{\varrho-3}+\ldots+y_1\varphi+y_0=\chi(\varphi),$$

so dass wir erhalten

$$\psi_1\cdot\chi(\varphi_1)+\psi_2\chi(\varphi_2)+\ldots+\psi_\varrho\chi(\varphi_\varrho)=A_0y_0+A_1y_1+\ldots \\ \ldots+A_{\varrho-2}y_{\varrho-2}+A_{\varrho-1}y_{\varrho-1}.$$

Um aus dieser Gleichung ψ_1 zu bestimmen und folglich ψ_2, ψ_3, $\ldots \psi_\varrho$ zu eliminieren, braucht man die y nur so zu wählen, dass wir erhalten $\chi(\varphi_2)=0, \quad \chi(\varphi_3)=0, \ldots \chi(\varphi_\varrho)=0; \quad \chi(\varphi_1)\neq 0.$

Nach dem dritten Kapitel § 51 genügen $\varphi_1, \varphi_2, \ldots \varphi_\varrho$ einer Gleichung ϱ^{ten} Grades

$$X(\varphi)=0,$$

deren Koefficienten rational in den c_α sind, und der Quotient

$$\frac{X(\varphi)}{\varphi-\varphi_1}=(\varphi-\varphi_2)(\varphi-\varphi_3)\ldots(\varphi-\varphi_\varrho) \\ =\varphi^{\varrho-1}-\beta_1\varphi^{\varrho-2}+\beta_2\varphi^{\varrho-3}-\ldots\pm\beta_{\varrho-1}$$

wird für $\varphi=\varphi_2, \varphi_3, \ldots \varphi_\varrho$ zu Null gemacht; für $\varphi=\varphi_1$ dagegen erhält man

$$X'(\varphi_1)=(\varphi_1-\varphi_2)(\varphi_1-\varphi_3)\ldots(\varphi_1-\varphi_\varrho);$$

diese Ableitung ist von Null verschieden, da bei von einander unabhängigen $x_1, x_2, \ldots x_n$ die Werte $\varphi_1, \varphi_2, \ldots \varphi_\varrho$ von einander verschieden sind. Wir können daher unseren Forderungen durch die Wahl

$$\chi(\varphi)=\frac{X(\varphi)}{\varphi-\varphi_1},$$

$$y_{\varrho-2}=-\beta_1, \quad y_{\varrho-3}=+\beta_2, \quad y_{\varrho-4}=-\beta_3, \ldots y_0=\pm\beta_{\varrho-1}$$

genügen. Setzt man nach dem dritten Kapitel § 51

$$X(\varphi)=\varphi^\varrho-\gamma_1\varphi^{\varrho-1}+\gamma_2\varphi^{\varrho-2}-\ldots\pm\gamma_\varrho,$$

so wird

$$\frac{X(\varphi)}{\varphi-\varphi_1}=\varphi^{\varrho-1}+[\varphi_1-\gamma_1]\varphi^{\varrho-2}+[\varphi_1^2-\varphi_1\gamma_1+\gamma_2]\varphi^{\varrho-3}+\ldots,$$

$$y_{\varrho-2}=\varphi_1-\gamma_1, \quad y_{\varrho-3}=\varphi_1^2-\varphi_1\gamma_1+\gamma_2, \quad y_{\varrho-4}=\varphi_1^3-\varphi_1^2\gamma_1+\varphi_1\gamma_2-\gamma_3,\ldots$$

und man erhält durch Einsetzung

$$\psi_1=\frac{R(\varphi_1)}{X'(\varphi_1)}.$$

Den Nenner wollen wir noch umformen. Es ist

$$X'(\varphi_1)\,.\,X'(\varphi_2)\ldots X'(\varphi_\varrho)$$

eine symmetrische Funktion und zwar, wie man aus dem Ausdrucke für $X'(\varphi_1)$ entnimmt, bis auf das Vorzeichen gleich der Diskriminante Δ_φ. Ferner ist

$$P) \qquad X'(\varphi_2).X'(\varphi_3)\dots X'(\varphi_\varrho)$$

eine symmetrische Funktion der Wurzeln der Gleichung

$$\frac{X(\varphi_1)}{\varphi-\varphi_1}=0$$

und daher rational durch die Koefficienten dieser Gleichung, d. h. die γ und φ_1, oder durch $c_1, c_2, \dots c_n, \varphi_1$ ausdrückbar. Erweitert man also den obigen Wert von ψ_1 mit diesem letzten Produkte P), so ergiebt sich

$$\psi_1=\frac{R_1(\varphi_1)}{\Delta_\varphi},$$

wo der Nenner rational und ganz in den c_α, der Zähler in den c_α und φ_1 ist.

Sollte der Zähler in Beziehung auf φ_1 den Grad $\varrho-1$ überschreiten, so ist eine zweite Umformung möglich. Man bilde nämlich

$$R_1(\varphi)=X(\varphi).Q(\varphi)+R_2(\varphi),$$

wobei $Q(\varphi)$ den Quotienten der Division $R_1(\varphi):X(\varphi)$ und $R_2(\varphi)$ den Rest derselben bezeichnet. Der Grad des letzteren übersteigt demgemäss die Zahl $\varrho-1$ nicht. Für alle Werte $\varphi_1, \varphi_2, \dots \varphi_\varrho$ ist $X(\varphi)=0$ und daher

$$R_1(\varphi_\lambda)=R_2(\varphi_\lambda) \quad (\lambda=1,2,3,\dots\varrho)$$

$$\psi_1=\frac{R_2(\varphi_1)}{\Delta_\varphi}.$$

Man hat damit den Satz:

Lehrsatz II. Drückt man die ϱ-wertige Funktion ψ_λ durch eine andere zu der Gruppe G_λ von ψ_λ gehörige Funktion φ_λ aus, so kann man ψ_λ als eine rationale gebrochene Funktion darstellen, deren Nenner die Diskriminante Δ_φ und daher rational und ganz in den $c_1, c_2, \dots c_n$ ist; der Zähler wird eine ganze, höchstens bis zum Grade $\varrho-1$ aufsteigende Funktion von φ_λ mit Koefficienten, welche ganz und rational in $c_1, c_2, \dots c_n$ sind.

§ 97. Die Umkehrung des ersten Lehrsatzes lautet:

Lehrsatz III. Sind zwei Funktionen gegenseitig rational durch einander ausdrückbar, so gehören sie zu derselben Gruppe.

In der That, wenn die beiden Gleichungen

$$\varphi=R_1(\psi), \quad \psi=R_2(\varphi)$$

bestehen, so zeigt die erstere, dass φ bei allen Substitutionen ungeändert bleibt, welche ψ nicht ändern, so dass die Gruppe von φ entweder die von ψ enthält oder mit ihr identisch ist; die zweite Gleichung zeigt umgekehrt, dass die Gruppe von ψ entweder die von φ enthält oder mit ihr identisch ist. Daraus folgt, dass die Gruppen beider Funktionen mit einander übereinstimmen.

Anmerkung. Scheinbar geht der in den Lehrsatz aufgenommene Begriff der Rationalität nicht in den Beweis ein. Es mag daher hier ausdrücklich darauf hingewiesen werden, dass dies dennoch in vollem Umfange der Fall ist. Denn wenn z. B. auch der Radikand eines der Ausdrücke

$$\sqrt{x_1^2 - x_1x_2 + x_2^2},\quad \sqrt{x_1^2 - 2x_1x_2 + x_2^2},\quad \sqrt{x_1^2 + 2x_1x_2 + x_2^2}$$

durch die Substitution $\sigma = (x_1x_2)$ ungeändert bleibt, so ist dadurch über das Vorzeichen der Wurzel und den Wert des Ausdrucks selbst nach der Ausführung der Transposition σ noch gar nichts bekannt. Bei rein substitutionen-theoretischen Betrachtungen lässt sich eine Entscheidung hierüber auch nicht fällen, und daher schränkt sich das Anwendungsgebiet dieser Lehren auf die rationalen Funktionen ein. Wenn, wie im zweiten und dritten der obigen Ausdrücke, die Wurzel sich wirklich in rationaler Form ausziehen lässt, wo man bezüglich

$$\pm(x_1 - x_2),\quad \pm(x_1 + x_2)$$

erhält, dann erkennt man, dass die Wirkung der Transposition σ sich durch Vorzeichenänderung beim zweiten Ausdrucke äussern wird, dass der dritte dagegen ungeändert bleibt. Über den ersten lässt sich nichts aussagen.

§ 98. Durch die Lehrsätze I) und III) ist ein algebraischer und ein gruppen-theoretischer Zusammenhang zwischen einer Reihe von Funktionen festgestellt. Wir rechnen alle rationalen ganzen Funktionen, zwischen denen eine gegenseitige rationale Ausdrückbarkeit besteht, d. h. alle diejenigen, welche zu einer und derselben Gruppe gehören, zu einer Gattung algebraischer Funktionen. Die Anzahl ϱ der Werte der Funktionen einer Gattung heisse die Ordnung der Gattung. Die verschiedenen Werte einer und derselben Funktion mögen zu unter einander konjugierten Gattungen gerechnet werden.*

Das Produkt aus der Ordnung einer Gattung und der Ordnung der zugehörigen Gruppe ist gleich $n!$, wenn n den Grad der Gruppe bezeichnet.

* L. Kronecker: Monatsber. d. Berl. Akad., 1879, S. 212.

Jede Funktion einer Gattung ϱ^{ter} Ordnung ist die Wurzel einer Gleichung ϱ^{ten} Grades, deren Koefficienten rational in den $c_1, c_2, \ldots c_n$ sind; die übrigen $\varrho - 1$ Wurzeln sind die konjugierten Funktionen.

Die Gruppen, welche zu konjugierten Gattungen gehören, haben, wenn $\varrho > 2$, $n > 4$ ist, ausser der Einheit keine gemeinsamen Substitutionen.

Für $\varrho = 2$ sind die beiden konjugierten Gattungen identisch.

Für $\varrho = 6$, $n = 4$ giebt es eine Gattung, die mit ihren fünf konjugierten Gattungen identisch ist.

§ 99. Bei dem Beweise in § 95 ist der Umstand, dass φ und ψ zu derselben Gattung gehören, nicht in vollem Umfange benutzt worden, sondern nur insoweit, als die dargestellte Funktion ψ für alle Substitutionen ungeändert bleibt, welche den Wert der darstellenden Funktion φ nicht ändern. Es könnten also, unbeschadet des Beweisganges, mehrere Werte ψ einander gleich werden, was bei den Werten von φ schon wegen des Auftretens der Diskriminante im Nenner nicht der Fall sein darf. Unter der allgemeineren Voraussetung, dass die Gruppe von ψ diejenige von φ umfasst, erhalten wir daher folgenden Satz:

Lehrsatz IV. Bleibt eine Funktion ψ für die Gruppe einer zweiten Funktion φ ungeändert, während das Umgekehrte nicht statt zu finden braucht, so kann ψ in der oben (Lehrsatz II) angegebenen Art durch φ rational dargestellt werden.

Wir sagen unter diesen Umständen, die Gattung der Funktion ψ sei unter der Gattung der Funktion φ enthalten. Dann ist also ψ rational durch φ darstellbar, aber nicht umgekehrt φ durch ψ. Die Gruppe der enthaltenden Funktion φ ist in der Gruppe der enthaltenen Funktion ψ enthalten. Zwischen den Begriffen des Enthaltens tritt also bei Gattung und Gruppe dieselbe Reciprocität ein wie oben zwischen den Ordnungszahlen ϱ und r.

Als Folgerungen schliessen wir an das Dargelegte folgende Sätze an:

Lehrsatz V. Es giebt stets eine Funktion, durch welche beliebig viele andere gegebene Funktionen rational ausgedrückt werden können; diese ist aus jenen linear darstellbar. Ihre Gattung enthält die Gattungen sämtlicher vorgelegten Funktionen.

In der That, es sind die gegebenen Funktionen $\varphi, \psi, \chi, \ldots$ durch

$$\bar{\omega} = \alpha\varphi + \beta\psi + \gamma\chi + \ldots$$

rational ausdrückbar, falls unter $\alpha, \beta, \gamma, \ldots$ willkürliche Parameter verstanden werden. Denn die Gruppe von ω wird durch diejenigen Substitutionen gebildet, welche $\varphi, \psi, \chi, \ldots$ gleichzeitig ungeändert lassen und daher den Gruppen von $\varphi, \psi, \chi, \ldots$ gemeinsam sind. Die Gruppe von $\bar{\omega}$ ist also in der jeder einzelnen Funktion $\varphi, \psi, \chi, \ldots$ enthalten, und aus diesem Umstande folgt der ausgesprochene Satz.

Einen speziellen Fall desselben erlangen wir, wenn die Gruppe von $\bar{\omega}$ sich auf die Einheit reduziert, $\bar{\omega}$ also eine $n!$-wertige Funktion wird. Durch diese Funktion $\bar{\omega}$ ist dann jede andere der n Elemente $x_1, x_2, \ldots x_n$ rational darstellbar; jede Gattung ist in der von $\bar{\omega}$ enthalten oder mit ihr identisch. Wir benennen diese Gattung die Galois'sche Gattung.

Lehrsatz VII. Jede rationale Funktion der n von einander unabhängigen Grössen $x_1, x_2, \ldots x_n$ lässt sich rational durch eine jede Funktion derselben n Grössen ausdrücken, welche $n!$ Werte besitzt; speziell also durch lineare Funktionen von der Form

$$\varphi = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n,$$

bei welcher die $\alpha_1, \alpha_2, \ldots \alpha_n$ willkürliche Parameter bedeuten.

§ 100. Wir wollen nun auch die Aufgabe zu lösen suchen, eine mehrwertige enthaltende Funktion φ durch eine wenigerwertige enthaltene Funktion ψ auszudrücken. Rational kann dies nach den eben durchgeführten Untersuchungen nicht geschehen. Die Aufgabe ist das Analogon und die Verallgemeinerung der im dritten Kapitel behandelten, welche die Darstellung einer ϱ-wertigen Funktion durch einwertige Funktionen forderte, und deren Lösung jene als Wurzel einer Gleichung ϱ^{ten} Grades mit symmetrischen Koefficienten lieferte.

Wir können daraus bereits das Resultat ablesen, welches hier zu erwarten ist. Es wird lauten:

Lehrsatz VIII. Ist die Gruppe einer $m.\varrho$-wertigen Funktion φ in der Gruppe einer ϱ-wertigen Funktion ψ enthalten, und sind

$$\varphi_1, \varphi_2, \ldots \varphi_m$$

diejenigen m Werte, welche φ_1 bei der Anwendung aller derjenigen Substitutionen annimmt, welche ψ_1 ungeändert lassen, so sind jene m Werte von φ die Wurzeln einer Gleichung m^{ten} Grades, deren Koefficienten rationale Funktionen von ψ_1 sind.

Es werden nämlich, wenn die Substitutionen der Gruppe

$$G = [s_1, s_2, \dots s_r], \quad r = \frac{n!}{\varrho}$$

von ψ_1 auf die symmetrischen Funktionen von $\varphi_1, \varphi_2, \dots \varphi_m$ in Anwendung gebracht werden, keine Wertänderungen dieser Funktionen eintreten, da sich nur die einzelnen Summanden unter einander vertauschen. Es folgt also insbesondere für die elementaren symmetrischen Funktionen

$$\begin{aligned}
\varphi_1 + \varphi_2 \quad &+ \dots + \varphi_m \quad &= A_1(\psi_1)\\
\varphi_1\varphi_2 + \varphi_1\varphi_3 &+ \dots + \varphi_{m-1}\varphi_m &= A_2(\psi_1)\\
&\dots\dots\dots\dots\dots\dots\dots\dots\\
\varphi_1\varphi_2 \dots \varphi_m &= A_m(\psi_1);
\end{aligned}$$

die A_λ sind hierbei rationale, im allgemeinen aber keine ganzen Funktionen von ψ_1. Man erhält infolge dieses Systems die Gleichung

$$(A_1) \quad \varphi^m - A_1(\psi_1).\varphi^{m-1} + A_2(\psi_1).\varphi^{m-2} - \dots \pm A_m(\psi_1) = 0,$$

deren Wurzeln $\varphi_1, \varphi_2, \dots \varphi_m$ sind, und die Gleichung

$$(A_\lambda) \quad \varphi^m - A_1(\psi_\lambda).\varphi^{m-1} + A_2(\psi_\lambda).\varphi^{m-2} - \dots \pm A_m(\psi_\lambda) = 0,$$

deren Wurzeln diejenigen m Werte von φ sind, welche dem Werte ψ_λ entsprechen, genau wie $\varphi_1, \varphi_2, \dots \varphi_m$ dem Werte ψ_1 entsprachen.

Die Nenner der einzelnen A_λ und daher der Generalnenner sämtlicher A_λ kann, wie oben bewiesen wurde (Lehrsatz II), stets als Teiler der Diskriminante Δ_ψ aufgestellt werden. Ist ψ eine einwertige Funktion, so fällt, wie schon aus dem dritten Kapitel § 51 erhellt, dieser Nenner ebenso wie der Begriff der Diskriminante weg.

§ 101. Ein besonderer Fall ist hier hervorzuheben: Sobald nämlich die enthaltene Gruppe der Funktion φ, welche H heissen möge, mit der Gruppe G von ψ vertauschbar ist (Kapitel 4 § 77), genügt es, eine einzige Wurzel der Gleichung (A_1) zu kennen, um alle rational bestimmen zu können.

Denn wenn

$$\varphi_1, \varphi_2, \varphi_3, \dots \varphi_m$$

die Wurzeln der Gleichung (A_1) und

$$H_1, H_2, H_3, \dots H_m$$

die zugehörigen Gruppen der φ sind, und wenn wir endlich eine beliebige Reihe solcher Substitutionen von G, welche φ_1 in die einzelnen Werte $\varphi_1, \varphi_2, \dots \varphi_m$ überführen, mit

$$\sigma_1 = 1, \sigma_2, \sigma_3, \dots \sigma_m$$

bezeichnen, so ist (Kapitel 3 § 45)

$$H_1 = \sigma_1^{-1} H_1 \sigma_1, \quad H_2 = \sigma_2^{-1} H_1 \sigma_2, \quad \dots \quad H_m = \sigma_m^{-1} H_1 \sigma_m.$$

Der Voraussetzung nach ist H_1 eine ausgezeichnete Untergruppe von G, da H_1 mit G vertauschbar ist; daher wird

d. h. $$G^{-1}H_1G^{+1} = H_1,$$

$$\sigma_2^{-1}H_1\sigma_2 = H_1, \quad \sigma_3^{-1}H_1\sigma_3 = H_1, \quad \ldots \quad \sigma_m^{-1}H_1\sigma_m = H_1.$$

Hieraus folgt nun in Verbindung mit den obigen Gleichungen für die H_λ,

$$H_1 = H_2 = H_3 = \ldots = H_m.$$

Die verschiedenen m Werte $\varphi_1, \varphi_2, \ldots \varphi_m$ gehören also zu einer und derselben Gruppe und sind daher rational durch einen beliebigen unter ihnen ausdrückbar, wie sich gemäss Lehrsatz I) ergiebt.

Die Gattung von ψ_1 war unter der von φ_1 enthalten; falls, wie hier die Gruppe H_1 von φ_1 nicht nur in der Gruppe G von ψ_1 enthalten ist, sondern als ausgezeichnete Untergruppe von G auftritt, nennen wir die Gattung von ψ_1 eine ausgezeichnete Untergattung der Gattung von φ_1.

Lehrsatz IX. Ist die Gruppe von φ_1 so beschaffen, dass durch eine Wurzel der Gleichung (A_1), z. B. durch φ_1, alle anderen $\varphi_2, \varphi_3, \ldots \varphi_m$ rational dargestellt werden können, dann ist die Gattung von ψ_1 eine ausgezeichnete Untergattung der Gattung von φ_1; und umgekehrt: wenn die Gattung von ψ_1 eine ausgezeichnete Untergattung derjenigen von φ_1 ist, so kann man alle Wurzeln der Gleichung (A_1) durch irgend eine derselben rational darstellen. Die Gruppe von φ_1 ist dann dieselbe wie die von $\varphi_2, \varphi_3, \ldots \varphi_m$ und eine ausgezeichnete Untergruppe der Gruppe von ψ_1.

§ 102. Wir untersuchen, wann und wodurch es ermöglicht werden kann, dass (A_1) eine binomische Gleichung wird. Wir nehmen dabei m als Primzahl an.

G_1 sei die Gruppe von ψ_1, H_1 die von φ_1. Soll (A_1) binomisch sein, müssen die Wurzeln $\varphi_1, \omega\varphi_1, \omega^2\varphi_1, \ldots \omega^{m-1}\varphi_1$ zu derselben Gruppe gehören. Es ist also notwendig, dass H_1 eine ausgezeichnete Untergruppe von G_1 ist. Jede Substitution von G_1 wirkt auf die $\varphi_1, \varphi_2, \ldots \varphi_m$ wie eine Substitution unter den φ selbst; G_1 ist also einer Gruppe der φ isomorph. Diese Gruppe ist transitiv und vom Grade m; nach S. 70 Lehrsatz II) ist ihre Ordnung durch m teilbar; nach S. 49 Lehrsatz X) enthält sie eine Substitution der Ordnung m. Bei m Elementen giebt es nur einen Typus

$$t = (\varphi_1\varphi_2 \ldots \varphi_m)$$

für eine solche Substitution. Die entsprechende Substitution τ aus G_1 vertauscht demnach $\varphi_1, \varphi_2, \ldots \varphi_m$ cyklisch. Da ferner τ^m dem t^m

entspricht, so wird τ^m alle Funktionen $\varphi_1, \varphi_2, \ldots \varphi_m$ ungeändert lassen, und es gehört also τ^m den Substitutionen von H_1 zu.

Unter diesen Festsetzungen kann man eine zur Gattung von φ_1 gehörige Funktion χ konstruieren, für welche (A_1) binomisch wird, also eine Funktion der Gattung von φ_1 finden, deren m^{te} Potenz zur Gattung von ψ_1 gehört. Dies geschieht folgendermassen: Wir verstehen unter ω eine primitive m^{te} Einheitswurzel und setzen

$$\chi_1 = \varphi_1 + \omega\varphi_2 + \omega^2\varphi_3 + \ldots + \omega^{m-1}\varphi_m.$$

Wenden wir auf diesen Ausdruck die verschiedenen Potenzen von t oder τ an, so ergiebt sich

$$\chi_2 = \varphi_2 + \omega\varphi_3 + \omega^2\varphi_4 + \ldots + \omega^{m-1}\varphi_1 = \omega^{-1}\cdot\chi_1$$
$$\chi_3 = \varphi_3 + \omega\varphi_4 + \omega^2\varphi_5 + \ldots + \omega^{m-1}\varphi_2 = \omega^{-2}\cdot\chi_1$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

und also

$$\chi_1^m = \chi_2^m = \ldots = \chi_m^m.$$

Jetzt ist zweierlei nachzuweisen: 1) dass χ_1 zur Gruppe H_1 von φ_1, 2) dass χ_1^m zur Gruppe G_1 von ψ_1 gehört. Dadurch ist der aufgestellte Satz bewiesen.

χ_1 bleibt für H_1 ungeändert, denn $\varphi_1, \varphi_2, \ldots \varphi_m$ thun es.

Bliebe χ_1 noch bei einer anderen Substitution ungeändert, so würde etwa

$$\varphi_1 + \omega\varphi_2 + \ldots + \omega^{m-1}\varphi_m = \varphi_{i_1} + \omega\varphi_{i_2} + \ldots + \omega^{m-1}\varphi_{i_m}$$
$$\omega^{m-1}(\varphi_m - \varphi_{i_m}) + \omega^{m-2}(\varphi_{m-1} - \varphi_{i_{m-1}}) + \ldots + (\varphi_1 - \varphi_{i_1}) = 0$$

folgen. Die letzte Gleichung hätte sonach mit der irreduktiblen Gleichung

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

eine und daher alle Wurzeln gemeinsam, d. h. es wäre

$$\varphi_1 - \varphi_{i_1} = \varphi_2 - \varphi_{i_2} = \ldots = \varphi_m - \varphi_{i_m}.$$

Konstruiert man nun φ_1 nach früheren Vorschriften als Summe von $\frac{n!}{m\,.\,\varrho}$ Summanden von der Form $x_1^{\alpha}x_2^{\beta}\ldots$ mit unbestimmten Exponenten (§ 31), so kann

$$\varphi_1 + \varphi_{i_2} = \varphi_2 + \varphi_{i_1}$$

nur dann stattfinden, wenn auf beiden Seiten dieselben Summanden stehen, da ja sonst eine Beziehung zwischen den x_λ konstituiert würde. Da ferner φ_1 nur Summanden enthält, welche von den übrigen $n! - \frac{n!}{m\,.\,\varrho}$ verschieden sind, so ist die letzte Gleichung nicht möglich. χ_1 gehört folglich zu H_1.

χ_1^m bleibt bei den Substitutionen von H_1 und bei t ungeändert. Es ist nun

$$G_1 = [H_1, t],$$

da die rechte Seite mindestens $m \cdot \frac{n!}{m.\varrho} = \frac{n!}{\varrho}$ Substitutionen enthält, welche sämtlich in der Gruppe G_1 der Ordnung $\frac{n!}{\varrho}$ enthalten sind. χ_1^m bleibt also für die Substitutionen von G_1 ungeändert; aber auch nur für sie. Denn sonst hätte χ_1^m weniger als ϱ Werte, und die m^{te} Wurzel χ_1 aus χ_1^m weniger als $m\varrho$ Werte, was dem Bewiesenen widerspräche.

§ 103. Die Angaben über G_1 und H_1 reichen also aus, um die Existenz von χ_1 zu beweisen. Sie sind ferner auch notwendig, wie nun gezeigt werden soll.

Es möge eine $m.\varrho$-wertige Funktion χ_1 der Gruppe H_1 bestehen, deren m^{te} Potenz χ_1^m nur ϱ-wertig wird und der Gruppe G_1 angehört. m bedeutet eine Primzahl.

Da die verschiedenen Werte von χ_1, welche unter dem Einflusse der Substitutionen von G_1 entstehen, sich nur durch Einheitswurzeln unterscheiden können, weil ihre m^{ten} Potenzen einander gleich sind, so gehören sie alle zu einer und derselben Gruppe. H_1 reproduziert sich demnach bei der Transformation durch irgend welche Substitutionen von G_1, und H_1 ist eine ausgezeichnete Untergruppe von G_1. Sind ferner die m Werte von χ_1, die sich nur durch Einheitswurzeln unterscheiden,

$$\chi_1, \omega\chi_1, \omega^2\chi_1, \ldots \omega^{m-1}\chi_1,$$

so giebt es, da alle χ_λ durch Transformation mit gewissen Substitutionen von G_1 aus χ_1 entspringen, eine solche Substitution τ, welche χ_1 in $\omega\chi_1$, also $\omega\chi_1$ in $\omega^2\chi_1$, $\omega^2\chi_1$ in $\omega^3\chi_1$, ... überführt und somit, wie bewiesen werden sollte, alle Werte von χ_1 cyklisch umsetzt.

Lehrsatz X. Damit in der durch die Gruppe H charakterisierten Gattung von Funktionen solche vorkommen, deren p^{te} Potenz zu der durch G charakterisierten Gattung gehören, ist es hinreichend und notwendig, dass H eine ausgezeichnete Untergruppe von G sei, oder was dasselbe ist, dass die zweite Gattung eine ausgezeichnete Untergattung der ersteren sei. Dabei werden in G Substitutionen vorkommen, welche alle in der Gattung von G enthaltenen, konjugierten Funktionen der Gattung von H cyklisch vertauschen.

Hieraus lässt sich leicht der Spezialfall herleiten:

Lehrsatz XI. Damit die Primzahlpotenz χ^p einer $p.\varrho$-wertigen Funktion nur ϱ Werte habe, ist es hinreichend und notwendig, dass es eine mit der Gruppe H von χ vertauschbare Substitution τ giebt, von welcher erst die p^{te} Potenz in H vorkommt.

Endlich liefert eine Erweiterung dieses Satzes folgendes wichtige Theorem:

Lehrsatz XII. Besteht für die Reihe

$$G,\ G_1,\ G_2,\ G_3,\ \ldots\ G_\nu$$

von Gruppen ein solcher Zusammenhang, dass jede vorhergehende $G_{\alpha-1}$ aus der folgenden G_α durch die Hinzunahme einer Substitution τ_α abgeleitet werden kann, welche mit G_α vertauschbar ist, und von der erst die p_α^{te}, eine Primzahlpotenz, in $G_{\alpha-1}$ enthalten ist, dann und nur dann kann man durch Auflösung einer Reihe binomischer Gleichungen der Grade $p_1,\ p_2,\ p_3,\ \ldots\ p_\nu$ eine $\varrho.p_1.p_2\ \ldots\ p_\nu$-wertige zu G_ν gehörige Funktion aus einer ϱ-wertigen zu G gehörigen ableiten.

§ 104. Bei der Darstellung einer Funktion durch eine andere zu derselben Gattung gehörige kamen wir zu rationalen, gebrochenen Ausdrücken, in deren Nenner ein Teiler der Diskriminante der darstellenden Funktion stand. Wenn wie bisher die $x_1,\ x_2,\ \ldots\ x_n$ als von einander völlig unabhängige Elemente angesehen werden, wird die Diskriminante einer beliebigen Funktion φ von Null verschieden sein, da ja ihre verschiedenen konjugierten Ausdrücke verschiedene Formen haben. Bestehen jedoch irgend welche Beziehungen zwischen den Elementen x, so ist es nicht mehr nötig, dass aus einer Verschiedenheit der Formen auch eine Verschiedenheit der Werte folge. Es wäre demgemäss, wenn in

$$f(x) \equiv x^n - c_1 x^{n-1} + c_2 x^{n-2} - \ldots \pm c_n$$

die Koefficienten spezielle Werte erhalten, wohl möglich, dass die Diskriminante

$$\Delta_\varphi = G(c_1,\ c_2,\ \ldots\ c_n)$$

Null wird. In diesem Falle wäre φ ungeeignet zur Darstellung anderer Funktionen derselben Gattung. Ja es wäre denkbar, dass alle Funktionen einer Gattung dieselbe Eigenschaft besässen. Es ist notwendig zu beweisen:

Lehrsatz XIII. Sind nicht zwei der Elemente x einander gleich, so giebt es, was auch sonst für Beziehungen unter

den x bestehen, stets Funktionen in jeder Gattung, deren Diskriminante von Null verschieden ist.

Den Beweis könnten wir ähnlich führen, wie jenen im § 30. Es ist aber bequemer, die dort erlangten Resultate, dass es unter den gemachten Annahmen $n!$-wertige Funktionen von der Form

$$\varphi = \alpha_0 + \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$$

giebt, hier zu benutzen. Sind nämlich die $n!$ Werte von φ von einander verschieden, so kann man α_0 derart wählen, dass sie auch verschiedene Moduln haben. Denn setzen wir

$$\varphi_\lambda = m_\lambda + \mu_\lambda \sqrt{-1} \quad (\lambda = 1, 2, \ldots n!),$$

so kann

$$\alpha' = p + q\sqrt{-1}$$

in der Weise angenommen werden, dass alle $n!$ Summen

$$\psi_\lambda = \varphi_\lambda + \alpha' = (m_\lambda + p) + (\mu_\lambda + q)\sqrt{-1} \quad (\lambda = 1, 2, \ldots n!)$$

verschiedene Moduln besitzen. Denn aus der Gleichung

$$(m_\lambda + p)^2 + (\mu_\lambda + q)^2 = (m_\varkappa + p)^2 + (\mu_\varkappa + q)^2$$

folgt bei völliger Willkürlichkeit von p und q

$$m_\lambda = m_\varkappa, \quad \mu_\lambda = \mu_\varkappa,$$

und man kann z. B. $p = q^2$ und q so gross annehmen, dass auch ein Spezialwert von q die Bedingungen erfüllt. Die ψ_λ seien der Grösse ihrer Moduln nach geordnet

$$\psi_1, \psi_2, \psi_3, \ldots \psi_{n!}; \quad (\text{mod. } \psi_\lambda > \text{mod. } \psi_{\lambda+1});$$

nun nehmen wir die ganze Zahl e so gross an, dass man erhält:

$$\psi_\lambda{}^e > \psi_{\lambda+1}{}^e + \psi_{\lambda+2}{}^e + \ldots + \psi_{n!}{}^e \quad (\lambda = 1, 2, \ldots, n! - 1).$$

Aus jeder Gleichung von der Form

$$\Psi) \qquad \psi_\alpha{}^e + \psi_b{}^e + \psi_c{}^e + \ldots = \psi_\alpha{}^e + \psi_\beta{}^e + \ldots$$

kann man dann folgern, die Indices a, b, c, ... seien den Indices α, β, ... gleich. Wendet man jetzt die r Substitutionen von G auf $\psi_1{}^e$ an und addiert die Resultate, so ist diese Summe

$$\bar{\omega} = \psi_1{}^e + \psi_{s_2}{}^e + \psi_{s_3}{}^e + \ldots + \psi_{s_r}{}^e$$

eine Funktion mit der gewünschten Eigenschaft. Erstens nämlich ändert sie sich für G nicht, und zweitens gehören alle Substitutionen, welche den Wert von $\bar{\omega}$ ungeändert lassen, zu G. Das Erstere ist klar; das Zweite schliessen wir aus der Folgerung, die sich an eine Gleichung von der Form Ψ) knüpfen lässt. $\bar{\omega}$ hat ϱ von einander verschiedene Werte; $\Delta_{\bar{\omega}}$ ist von 0 verschieden.

Sechstes Kapitel.

Die Anzahl der Werte ganzer Funktionen.

§ 105. Wir haben bisher nur vereinzelte Sätze über die Existenz mehrwertiger Funktionen kennen gelernt. Ein- und zweiwertige Funktionen einerseits ($\varrho = 1, 2$); $n!$-wertige andererseits ($\varrho = n!$) bilden die untere und die obere Grenze für die minder- oder mehrwertigen Funktionen. Ein wichtiges negatives Resultat wurde im dritten Kapitel § 42 abgeleitet, dass nämlich ϱ keinen Wert annehmen kann, der nicht $n!$ teilt. Weiter ist uns noch nichts bekannt. Wir können aber leicht durch die Bildung von intransitiven und von imprimitiven Gruppen eine Fülle spezieller Resultate erhalten. Nur sind alle diese positiv, während die negativen, durch welche etwas über die Nichtexistenz von Funktionen ausgesagt wird, gerade die interessanten sind.

Die allgemeine Konstruktion der intransitiven Gruppen würde, wie in § 90 sich zeigte, ein genaueres Eingehen auf den Isomorphismus in weitestem Sinne fordern. Wir begnügen uns damit, die einfachsten Bildungen anzugeben. Sind $n = a + b + c + \ldots$ Elemente vorhanden, und bilden wir aus a derselben eine symmetrische oder alternierende Gruppe, ebenso aus b anderen von denselben eine symmetrische oder alternierende Gruppe u. s. w., so erhalten wir durch die Multiplikation der Substitutionen dieser einzelnen Gruppen unter einander eine intransitive Gruppe des Grades n und der Ordnung

$$r = \varepsilon . a! b! c! \ldots,$$

wo $\varepsilon = 1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots$ ist, je nachdem man bei der Gruppenbildung keine, eine, zwei, drei, ... alternierende und im übrigen nur symmetrische Gruppen verwendet hat. Es wird dementsprechend

$$\varrho = \frac{n!}{\varepsilon . a! b! c! \ldots}$$

die Anzahl der Werte der zugehörigen Funktionen sein. Ist nur n gegeben, so kann man also Funktionen finden, die einem beliebigen in der angegebenen Weise gebildeten ϱ genügen. Nehmen wir z. B. $n = 5$, so lassen sich aufstellen:

$a = 5;$ $\quad \varepsilon = 1,$ $\quad \varrho = 1;$ $\quad \varphi_1 = x_1 x_2 x_3 x_4 x_5.$

$a = 5;$ $\quad \varepsilon = \frac{1}{2},$ $\quad \varrho = 2;$ $\quad \varphi_2 = (x_1 - x_2)(x_1 - x_3) \ldots (x_4 - x_5)$

$a = 4,$ $\quad b = 1;$ $\quad \varepsilon = 1,$ $\quad \varrho = 5;$ $\quad \varphi_3 = x_1 x_2 x_3 x_4.$

$a=4,\ b=1;\qquad \varepsilon=\frac{1}{2},\ \varrho=10;\quad \varphi_4=(x_1-x_2)(x_1-x_3)(x_1-x_4)(x_2-x_3)(x_2-x_4)(x_3-x_4).$

$a=3,\ b=2;\qquad \varepsilon=1,\ \varrho=10;\quad \varphi_5=x_1x_2x_3+x_4x_5.$

$a=3,\ b=2;\qquad \varepsilon=\frac{1}{2},\ \varrho=20;\quad \varphi_6=(x_1-x_2)(x_1-x_3)(x_2-x_3)+x_4x_5.$

$\varphi_7=x_1x_2x_3+x_4-x_5.$

$a=3,\ b=2;\qquad \varepsilon=\frac{1}{4},\ \varrho=40;\quad \varphi_8=(x_1-x_2)(x_1-x_3)(x_2-x_3)+x_4-x_5.$

$a=3,\ b=1,\ c=1;\quad \varepsilon=1,\ \varrho=20;\quad \varphi_9=x_1x_2x_3.$

. . . . . .

Die imprimitiven Gruppen, deren allgemeine Konstruktion oben in § 73 angegeben worden ist, geben in gleicher Weise Gelegenheit zur Bildung von Gruppen und damit von Funktionen mit gewissen Wertanzahlen. Für $n=6$ erhielte man z. B., je nachdem man zwei Systeme der Imprimitivität von je drei Elementen oder drei Systeme von je zwei Elementen annimmt, mehrere Gruppen, deren Kenntnis nur von derjenigen aller Gruppen der Grade zwei und drei abhängt.

§ 106. Allgemeine und fundamental wichtige Resultate erhält man aber auf diesem Wege nicht. Wir greifen die Untersuchung daher von einer anderen Seite an, welche uns zuerst eine Umwandlung unserer Frage erlauben wird.

Ist die ϱ-wertige Funktion φ_1 mit ihrer Gruppe G_1 gegeben, so bilden wir dieselbe Tabelle, welche wir bereits in § 41 benutzten. Diese enthält in ϱ Zeilen alle $n!$ Substitutionen; in der ersten diejenigen, welche φ_1 nicht ändern, in der zweiten diejenigen, welche φ_1 in φ_2 umwandeln u. s. f. Die Tabelle lautet

$$\begin{array}{llll}
s_1=1, & s_2, & s_3, \ \ldots & s_r; \quad G_1 \\
\sigma_2, & s_2\sigma_2, & s_3\sigma_2, \ \ldots & s_r\sigma_2; \quad G_1\cdot\sigma_2 \\
\sigma_3, & s_2\sigma_3, & s_3\sigma_3, \ \ldots & s_r\sigma_3; \quad G_1\cdot\sigma_3 \\
\cdots & \cdots & \cdots & \cdots \\
\sigma_\varrho, & s_2\sigma_\varrho, & s_3\sigma_\varrho, \ \ldots & s_r\sigma_\varrho; \quad G_1\cdot\sigma_\varrho.
\end{array}$$

Wir untersuchen die Verteilung der Substitutionen eines bestimmten Typus innerhalb dieser Tabelle.

A) Es giebt $n-1$ Transpositionen von der Form (x_1x_α); $\alpha=2,3,\ldots n$. Ist also $\varrho<n$, und kommt in der Gruppe G_1 von φ_1 keine Transposition von der Form (x_1x_α) vor, so sind diese $n-1$ Transpositionen auf höchstens $n-2$ Zeilen verteilt; demnach müssen in einer der auf die erste folgenden Zeilen mindestens zwei derartige Transpositionen auftreten. Es mögen die folgenden sein:

$$s_\alpha \sigma_\lambda = (x_1 x_a), \quad s_\beta \sigma_\lambda = (x_1 x_b),$$

dann ergiebt sich, dass eine Kombination beider

$$(x_1 x_a x_b) = (x_1 x_a)(x_1 x_b) = s_\alpha \sigma_\lambda (s_\beta \sigma_\lambda)^{-1} = s_\alpha \sigma_\lambda \sigma_\lambda^{-1} s_\beta^{-1} = s_\alpha s_\beta^{-1} = s_\gamma$$

in G_1 vorkommt. Es muss folglich für $\varrho < n$ in G_1 entweder eine Transposition oder eine Cirkularsubstitution dritter Ordnung vorkommen, welche ein vorgeschriebenes Element x_1 enthält. Dasselbe gilt für jedes andere x_λ.

B) Es giebt $\frac{n(n-1)}{2}$ Substitutionen von der Form $(x_\alpha x_\beta)$, $(\alpha \neq \beta = 1, 2, \ldots n)$. Ist also $\varrho \leqq \frac{n(n-1)}{2}$, und kommt in der ersten Zeile der Tabelle keine Transposition $(x_\alpha x_\beta)$ vor, so treten in irgend einer anderen Zeile sicher mindestens zwei auf. Stimmen diese in einem Elemente überein, wie etwa $(x_\alpha x_\beta)$, $(x_\alpha x_\gamma)$, so erhalten wir, wie soeben durch Multiplikation eine in G_1 enthaltene Substitution $(x_\alpha x_\beta x_\gamma)$; stimmen die beiden Transpositionen in keinem Elemente überein $(x_\alpha x_\beta)$, $(x_\gamma x_\delta)$, so ergiebt sich durch Kombination eine in G_1 enthaltene Substitution $s_\lambda = (x_\alpha x_\beta)(x_\gamma x_\delta)$. G_1 enthält also jedenfalls eine Substitution von nicht mehr als vier Elementen.

C) Es giebt $(n-1)(n-2)$ Substitutionen von der Form $(x_1 x_\alpha x_\beta)$, $(\alpha \neq \beta = 2, 3, \ldots n)$. Ist also $\varrho \leqq (n-1)(n-2)$, und kommt in G_1 keine Substitution der angegebenen Form vor, so erhält man in einer anderen Zeile der Tabelle mindestens zwei; eine Kombination derselben zeigt, dass G_1 Substitutionen von drei, vier oder fünf Elementen enthalten wird.

So erhält man eine Reihe von Sätzen, von denen wir einige zusammenstellen:

Lehrsatz I. 1) Ist die Anzahl ϱ der Werte einer Funktion nicht grösser als $n-1$, so enthält die Gruppe der Funktion eine Substitution von höchstens drei Elementen, unter denen sich ein gegebenes befindet. 2) Ist die Anzahl ϱ der Werte einer Funktion nicht grösser als $\frac{n(n-1)}{2}$, so enthält die Gruppe der Funktion eine Substitution von höchstens vier Elementen. 3) Ist die Anzahl ϱ der Werte einer Funktion nicht grösser als $\frac{n(n-1)(n-2)}{3}$, so enthält die Gruppe der Funktion eine Substitution von höchstens sechs Elementen. 4) Ist die Anzahl der Werte einer Funktion nicht grösser als

$\frac{n(n-1)(n-2)\ldots(n-k+1)}{k}$, so enthält die zugehörige Gruppe eine Substitution von höchstens $2k$ Elementen. 5) Ist die Anzahl der Werte einer Funktion nicht grösser als $(n-1)(n-2)\ldots(n-k+1)$, so enthält die zugehörige Gruppe eine Substitution von höchstens $2k-1$ Elementen, unter denen sich ein vorgeschriebenes befindet, so dass also mindestens $\frac{n}{2k-1}$ derartige Substitutionen vorhanden sind.

Die Frage nach der Anzahl der Werte mehrwertiger Funktionen ist infolge dieser Resultate auf eine andere, nämlich auf die nach der Existenz von Gruppen reduziert, welche Substitutionen mit einer gewissen Minimalanzahl von Elementen besitzen.

§ 107. Stellen wir das erste der Resultate unseres Lehrsatzes mit früheren Sätzen zusammen, so erhalten wir den Beweis eines wichtigen Theorems.

Wir wissen aus dem vierten Kapitel Lehrsatz I), dass die Ordnung einer intransitiven Gruppe höchstens $(n-1)!$ ist; folglich ist die Anzahl der Werte einer Funktion mit intransitiver Gruppe mindestens $\frac{n!}{(n-1)!} = n$; für eine solche Funktion kann also ϱ nicht kleiner als n sein. Aus Lehrsatz XII) desselben Kapitels ersehen wir, dass die Ordnung einer imprimitiven Gruppe höchstens $2!\left(\frac{n!}{2}\right)^2$ ist; folglich ist die Anzahl der Werte einer Funktion mit imprimitiver Gruppe mindestens $\frac{n!}{2!\frac{n}{2}!\frac{n}{2}!}$; diese Zahl ist für $n=4$ kleiner als n, nämlich gleich drei; für $n>4$ dagegen ist sie grösser als n. Also kann für $n>4$ bei einer solchen Funktion ϱ nicht kleiner als n sein. Bei primitiven Gruppen folgt aber aus dem vierten Kapitel Lehrsatz XIII) wegen des ersten Resultates unseres Lehrsatzes aus § 106, dass für $\varrho<n$ die Gruppe alternierend oder symmetrisch, ϱ also $=2$ oder $=1$ ist. Die imprimitive Gruppe, welche zu $n=4$, $\varrho=3$, $r=8$ gehört, ist uns bekannt; es ist die schon vielfach besprochene. So folgt:

Lehrsatz II. Ist die Anzahl ϱ der Werte einer Funktion nicht grösser als $n-1$, so ist entweder $\varrho=1$ oder $=2$; die Gruppe der Funktion wird also die symmetrische oder die alternierende sein. Eine Ausnahme findet nur für $n=4$, $\varrho=3$

$r = 8$ statt bei allen den zur Gruppe von $\varphi = x_1 x_2 + x_3 x_4$ gehörigen Funktionen.

§ 108. Wir wollen denselben Satz noch einmal von einem anderen Beweisgrunde aus ableiten.*

Es sei φ eine $\varrho < n$-wertige Funktion, deren Werte wir durch

$$\varphi_1, \varphi_2, \varphi_3, \cdots \varphi_\varrho$$

bezeichnen. Wendet man auf diese Reihe irgend welche Substitutionen an, so vertauschen sich lediglich die ϱ Werte untereinander, wie wir bereits früher sahen. Wendet man insbesondere auf diese Reihe eine Substitution der zu φ_1 gehörigen Gruppe G_1 an, so vertauschen sich die ϱ Werte derart untereinander, dass φ_1 dabei seinen Platz nicht verlässt. Alle $r = \frac{n!}{\varrho} > (n-1)!$ Substitutionen von G_1 wirken also in der Weise, dass sie nur $\varphi_2, \varphi_3, \ldots \varphi_\varrho$ in andere Stellungen bringen. Solcher Stellungen giebt es, da $\varrho < n$ ist, höchstens $(\varrho - 1)! \leqq (n-2)!$ verschiedene; folglich werden unter den $r > (n-1)!$ Substitutionen von G_1 mindestens zwei dieselben Änderungen der $\varphi_2, \varphi_3, \ldots \varphi_\varrho$ unter einander hervorbringen. σ, τ seien solche Substitutionen; dann wird $\sigma . \tau^{-1}$ alle φ an ihren Plätzen lassen. Es ist also $\sigma . \tau^{-1}$ eine von der Einheit verschiedene Substitution, welche alle $\varphi_1, \varphi_2, \ldots \varphi_\varrho$ ungeändert lässt und daher zu den Gruppen $G_1, G_2, \ldots G_\varrho$ gleichzeitig gehört. Nach dem dritten Kapitel Lehrsatz XI) erkennt man hieraus die Richtigkeit des zu beweisenden Satzes.

§ 109. Sucht man nun, um zu allgemeineren Fragen zurückzukehren, alle Funktionen, deren Wertezahl eine gewisse, vom Grade n abhängende obere Grenze nicht überschreitet, so können wir, was im vorigen Paragraphen für einen besonderen Fall geleistet wurde, gleich allgemein abthun, nämlich die Betrachtung der weniger wichtigen intransitiven und imprimitiven Gruppen. Wir gehen dabei auf die im vierten Kapitel gegebenen Bildungen zurück.

Für die intransitiven Gruppen haben wir als Maximalordnungen erhalten:

1) $r = (n-1)!$, wenn $(n-1)$ Elemente eine transitive, symmetrische Gruppe bilden und das letzte Element sich an der Substitutionenbildung gar nicht beteiligt. Es wird $\varrho = n$.

---

* L. Kronecker: Monatsber. d. Berl. Akad., 1879, S. 211.

2) $r = \frac{(n-1)!}{2}$, wenn $(n-1)$ Elemente eine alternierende Gruppe bilden und das letzte Element sich an der Substitutionenbildung gar nicht beteiligt. Es wird $\varrho = 2n$.

3) $r = 2!\,(n-2)!$, wenn $(n-2)$ Elemente eine symmetrische Gruppe, die beiden anderen eine Transposition bilden und beide Gruppen mit einander multipliziert werden. Es wird $\varrho = \frac{n(n-1)}{2}$.

4) $r = (n-2)!$, wenn entweder $(n-2)$ Elemente eine alternierende Gruppe, die beiden anderen eine Transposition bilden und beide Gruppen mit einander multipliziert werden; oder wenn $(n-2)$ Elemente eine symmetrische Gruppe bilden und die beiden anderen sich an der Substitutionenbildung nicht beteiligen. Es wird $\varrho = n(n-1)$.

So kann man fortfahren.

Für imprimitive Gruppen erhält man:

1) $r = 2!\left(\frac{n!}{2}\right)^2$, wenn man zwei Systeme der Imprimitivität von je $\frac{n}{2}$ Elementen hat, aus jedem die symmetrische Gruppe bildet, und beide Systeme auf alle Arten mit einander verbindet. Es wird $\varrho = \frac{n!}{2 \cdot \left(\frac{n!}{2}\right)^2}$; für $n = 4, 6, 8, \ldots$ wird $\varrho = 3, 10, 35, \ldots$

2) $r = 3!\left(\frac{n!}{3}\right)^3$, wenn man drei Systeme der Imprimitivität bildet, jedes zu $\frac{n}{3}$ Elementen, von jedem die symmetrische Gruppe aufstellt und diese drei auf alle möglichen Arten kombiniert. Es wird $\varrho = \frac{n!}{3!\left(\frac{n!}{3}\right)^3}$; für $n = 6, 9, 12, \ldots$ erhält man $\varrho = 15, 280, 5770, \ldots$

3) $r = 3 \cdot \left(\frac{n!}{3}\right)^3$, wenn die obigen drei Systeme der Imprimitivität nur gemäss der Gruppe $\Gamma = [1, (y_1 y_2 y_3), (y_1 y_3 y_2)]$ (vergl. § 73) kombiniert werden. Es wird $\varrho = \frac{n!}{3 \cdot \left(\frac{n!}{3}\right)^3}$; für $n = 6, 9, 12, \ldots$ erhält man $\varrho = 30, 560, 11540, \ldots$

Wie man sieht, wachsen die Werte von ϱ in ausserordentlich schneller Weise.

§ 110. Wir untersuchen nun im Anschlusse an die Resultate von § 106 die primitiven Gruppen, welche Substitutionen von vier, aber keine von nur drei oder zwei Elementen enthalten.

Eine der vorkommenden Substitutionen von vier Elementen sei $s = (x_a x_b)(x_c x_d)$. Eine solche muss vorhanden sein, denn aus dem Vorkommen von $\sigma = (x_\alpha x_\beta x_\gamma x_\delta)$ würde durch Quadrierung der aufgestellte Typus s folgen.

Es sei $$s_5 = (x_1 x_2)(x_3 x_4)$$
die in der primitiven Gruppe G vorkommende Substitution von vier Elementen, welche wir zum Ausgangspunkte wählen. Wir transformieren s_5 durch alle Substitutionen von G und kommen dadurch nach der Methode von § 74 zu einer Reihe von Substitutionen desselben Typus, durch welche x_1, x_2, x_3, x_4 mit allen übrigen Elementen in Verbindung treten. Es sind also in G Substitutionen vorhanden, welche s_5 ähnlich sind, und welche ausser einigen der alten Elemente x_1, x_2, x_3, x_4 noch neue Elemente x_5, x_6, x_7, ... enthalten, welche sie mit jenen in Verbindung setzen.

Dies ist auf dreierlei Arten möglich, je nachdem ein neues, zwei oder drei neue Elemente mit drei, zwei oder einem alten Elemente verbunden auftreten. Achtet man darauf, dass es lediglich auf die Art der Verbindung der alten mit den neuen Elementen ankommt, nicht auf die Benennung derselben, so erkennt man, dass es nur fünf typische Formen geben kann, nämlich folgende:

I) $(x_1 x_2)(x_3 x_5)$, $(x_1 x_3)(x_2 x_5)$,
II) $(x_1 x_5)(x_2 x_6)$, $(x_1 x_5)(x_3 x_6)$,
III) $(x_1 x_5)(x_6 x_7)$.

Bei der ersten von diesen macht es z. B. keinen Unterschied, ob man schreibt $$(x_1 x_2)(x_4 x_5),\quad (x_3 x_4)(x_1 x_5),\quad (x_3 x_4)(x_2 x_5);$$
bei der letzten, ob man x_1 mit x_2, x_3, x_4 vertauscht u. s. w.

Die erste und die fünfte dieser Möglichkeiten fallen sofort weg, da man aus ihnen Schlüsse ziehen kann, welche gegen die Annahmen über die Natur unserer Gruppen verstossen. Man findet nämlich, dass
$$(x_1 x_2)(x_3 x_4) \cdot (x_1 x_2)(x_3 x_5) = (x_3 x_4 x_5)$$
$$[(x_1 x_2)(x_3 x_4) \cdot (x_1 x_5)(x_6 x_7)]^2 = (x_1 x_5 x_2)$$
nur drei Elemente enthalten, während doch derartige Substitutionen in unseren Gruppen nicht vorkommen sollten.

Es bleiben daher nur drei Fälle zurück, welche wir der Reihe nach zu untersuchen haben: je nachdem G ausser s_5 noch eine der drei Substitutionen enthält

A) $(x_1 x_3)(x_2 x_5)$,
B) $(x_1 x_5)(x_2 x_6)$,
C) $(x_1 x_5)(x_3 x_6)$.

§ 111. A) Es kommt in der primitiven Gruppe vor

$$s_5 = (x_1 x_2)(x_3 x_4), \quad s_4 = (x_1 x_3)(x_2 x_5).$$

Folglich findet sich in ihr auch

$$t = s_5 s_4 = (x_1 x_5 x_2 x_3 x_4),$$

und die Transformierten von s_5 durch die Potenzen von t kommen in G gleichfalls vor

$$s_1 = (x_2 x_3)(x_4 x_5), \quad s_2 = (x_1 x_4)(x_3 x_5), \quad s_3 = (x_1 x_5)(x_2 x_4),$$
$$s_4 = (x_1 x_3)(x_2 x_5), \quad s_5 = (x_1 x_2)(x_3 x_4).$$

Da t eine Cirkularsubstitution der Primzahlordnung $p = 5$ ist, so ist nach § 75 die Gruppe G des Grades n mindestens $(n-4)$-fach transitiv.

Ist $n \geqq 7$, so wird G alternierend oder symmetrisch sein. Dann existiert also eine Gruppe mit den verlangten Eigenschaften nicht.

Denn für $n \geqq 7$ ist G mindestens dreifach transitiv. Es giebt also in G eine Substitution τ, welche x_1 nicht umstellt, x_2 durch x_6 und x_3 durch x_7 ersetzt. Transformiert man durch diese die Substitution s_5, so entsteht

$$s' = \sigma^{-1} s_5 \sigma = (x_1 x_6)(x_7 x_a).$$

Wenn x_a zu den Elementen x_2, x_3, x_4, x_5 gehört, dann hat s' mit s_a nur ein Element gemeinsam. Gehört x_a zu den Elementen x_8, x_9, ..., so hat s' mit jeder der Substitutionen s_1, s_2, ... s_5 nur ein Element gemeinsam. Beide Annahmen führen auf die im vorigen Paragraphen besprochene und beseitigte Möglichkeit III).

Es sind, wie man leicht erkennt, für $n = 4$ nur zwei entsprechende, aber imprimitive Gruppen vorhanden. Gruppen des Typus A) giebt es also höchstens für $n = 5$ oder $n = 6$.

§ 112. B) In diesem Falle kommen in G vor

$$s_5 = (x_1 x_2)(x_3 x_4), \quad \tau = (x_1 x_5)(x_2 x_6)$$

und folglich auch die Kombination beider

$$v = s_5^{-1} \tau s_5 = (x_1 x_6)(x_2 x_5).$$

Durch diese drei Substitutionen sind die sechs vorkommenden Elemente x_1, x_2, ... x_6 noch nicht transitiv mit einander verbunden, da zwischen x_3, x_4 und x_1, x_2, x_5, x_6 noch kein Zusammenhang besteht. Es muss also eine Substitution des Typus $(x_\alpha x_\beta)(x_\gamma x_\delta)$ in der Gruppe vorkommen, welche x_1, x_2, x_5, x_6 mit anderen Elementen verbindet. Enthielte diese Substitution drei der Elemente x_1, x_2, x_5, x_6 und nur ein neues, so würde sie mit v drei Elemente gemeinsam haben. Man

käme also entweder auf den Typus A) oder auf die erste der beiden Möglichkeiten von I) in § 110 zurück. Das Eine ist erledigt, das Andere beseitigt. Wenn die neue Substitution nur eins der Elemente x_1, x_2, x_5, x_6 und drei andere enthielte, so träte sie mit v zum Typus III) aus § 110 zusammen. Auch dies ist zu verwerfen, und es bleibt nur übrig, dass zwei der vier Elemente mit zwei neuen verbunden vorkommen. Die geforderte Substitution muss also eine der Formen haben

$$(x_1x_a)(x_2x_b),\quad (x_1x_a)(x_5x_b),\quad (x_1x_a)(x_6x_b),$$
$$(x_2x_a)(x_5x_b),\quad (x_2x_a)(x_6x_b),\quad (x_5x_a)(x_6x_b).$$

Von diesen stehen die erste, dritte, vierte und fünfte zu τ, die zweite, dritte, fünfte und sechste zu v in der durch C) charakterisierten Verbindung.

Die Behandlung von B) führt also notwendig auf C), so dass alle zu B) gehörigen Gruppen bei der Untersuchung der zu C) gehörigen sich finden müssen. Wir können uns daher auf diese letzten beschränken.

§ 113. C) In diesem Falle kommen in der gesuchten Gruppe

$$\sigma_1 = (x_1x_2)(x_3x_4),\quad \sigma_2 = (x_1x_5)(x_3x_6),\quad \sigma_3 = \sigma_1^{-1}\sigma_2\sigma_1 = (x_2x_5)(x_4x_6)$$

vor.

Wir behandeln zuerst den Fall $n = 6$.

Die Elemente x_1, x_2, x_5 sind noch nicht mit x_3, x_4, x_6 verbunden. Eine Verbindung nach dem Typus $(x_\alpha x_\beta)(x_\gamma x_\delta)$ muss stattfinden. x_α möge zu den drei Elementen x_1, x_2, x_5 gehören. Wäre x_α gleich x_2 oder gleich x_5, so transformierte man durch σ_1 oder σ_2 und erhielte dann $(x_1x_b)(x_cx_d)$, so dass also $\alpha = 1$ vorausgesetzt werden darf. Dann sind die möglichen Substitutionen folgende:

$\alpha)$ $(x_1x_2)(x_5x_m)$, $(x_1x_5)(x_2x_m)$, $(x_2x_5)(x_1x_m)$, $\quad m = 3, 4, 6.$

$\beta)$ $(x_1x_m)(x_nx_p)$, $\quad m, n, p = 3, 4, 6.$

$\gamma)$ $(x_1x_m)(x_2x_n)$, $(x_1x_m)(x_5x_n)$, $\quad m, n = 3, 4, 6.$

Die drei ersten Substitutionen sind zu verwerfen, da ihre Produkte in σ_1, σ_2, σ_3 auf § 110, I) oder auf Substitutionen mit nur drei Elementen führen. Bei der Substitution der zweiten Zeile findet dasselbe statt. Es bleiben also nur noch übrig, je nach den Werten von m, n:

$$(x_1x_3)(x_2x_4),\quad (x_1x_4)(x_2x_3),$$
$$(x_1x_3)(x_2x_6),\quad (x_1x_6)(x_2x_3),$$
$$(x_1x_4)(x_2x_6),\quad (x_1x_6)(x_2x_4);$$
$$(x_1x_3)(x_5x_4),\quad (x_1x_4)(x_5x_3),$$
$$(x_1x_3)(x_5x_6),\quad (x_1x_6)(x_5x_3),$$
$$(x_1x_4)(x_5x_6),\quad (x_1x_6)(x_5x_4).$$

Die zweite und vierte Zeile muss ausgeschlossen werden, da ihre Substitutionen mit σ_1, die dritte und sechste, weil ihre Substitutionen mit σ_3 je drei Elemente gemeinsam haben.

Die erste Zeile steht zu σ_1 in derselben Beziehung wie die fünfte zu σ_2; wir können uns also ohne Beschränkung mit der Betrachtung der ersten allein beschäftigen.

Jede ihrer Substitutionen ruft mit σ_1 multipliziert die andere hervor. Man kommt also zu allen etwa für $n = 6$ vorhandenen Gruppen, wenn man

$$\sigma_4 = (x_1 x_3)(x_2 x_4)$$

zu σ_1, σ_2, σ_3 hinzunimmt.

§ 114. Wenn der Grad der Gruppe grösser ist als 6, so können in den drei Zeilen $\alpha)$, $\beta)$, $\gamma)$ des vorigen Paragraphen die Indices m, n, p auch Werte annehmen, welche grösser sind als 6. Man erkennt aber sofort wieder, dass die drei Annahmen von $\alpha)$ jedenfalls auf Widersprüche führen. Bei $\beta)$ und $\gamma)$ kann man zu Substitutionen gelangen, welche die Bedingungen, denen genügt werden soll, nicht verletzen. Die Durchführung zeigt, dass, wie dies auch immer geschehe, eine Kombination der erhaltenen Substitutionen zu einer Cirkularsubstitution von sieben Elementen führt.

Folglich ist nach § 75 die Gruppe mindestens $(n-6)$-fach transitiv.

Wäre $n \geqq 9$, so wäre G mindestens 3-fach transitiv, enthielte also eine Substitution, welche x_1 nicht umsetzte, x_2 und x_3 mit einander vertauschte. Wendet man diese Substitution auf σ_1 an, so entsteht

$$\sigma' = (x_1 x_3)(x_2 x_a),$$

also, da σ' mit σ drei Elemente gemeinsam hat und um der Möglichkeit A) zu entgehen, $x_a = x_4$. Es wird also σ' gleich dem σ_4 des vorigen Paragraphen.

Danach ist die Untergruppe, welche $x_1, x_2, \ldots x_6$ enthält, bereits einfach transitiv. Nimmt man dazu die Cirkularsubstitution mit sieben Elementen, so erhält man eine zweifach transitive Gruppe und erkennt aus § 76, dass G mindestens $(n-5)$-fach, also für $n \geqq 9$ mindestens 4-fach transitiv ist. G enthält also ein

$$\tau = (x_1)(x_2 x_3)(x_4 x_5 \ldots)$$
$$\tau^{-1}\sigma_1\tau = (x_1 x_3)(x_2 x_5),$$

so dass man auf jeden Fall zum Typus A) gelangt. Für $n \geqq 9$ giebt es also keine Gruppen der verlangten Eigenschaften.

Lehrsatz III. Übersteigt der Grad einer Gruppe, welche Substitutionen von vier, aber keine von drei oder zwei Ele-

menten enthält, die Zahl 8, so ist die Gruppe intransitiv oder imprimitiv.

Verbindet man hiermit die Resultate der §§ 106 und 109, so folgt:

Lehrsatz IV. Ist die Anzahl ϱ der Werte einer Funktion nicht grösser als $\frac{1}{2}n(n-1)$, so wird dieselbe für $n>8$ symmetrisch in $n-2$ Elementen einerseits und in den beiden übrigen andrerseits sein; oder es wird für sie $\varrho=2n$, und die Funktion ist alternierend in $(n-1)$ Elementen; oder es wird $\varrho=n$ und die Funktion ist symmetrisch in $(n-1)$ Elementen; oder ϱ ist $=1, 2$, und die Funktion ist symmetrisch respektive alternierend in allen n Elementen.*

§ 115. Wir schieben jetzt einen Hilfssatz ein, dessen wir zum Beweise eines allgemeineren Theorems bedürfen.**

Nach § 75 Lehrsatz XVI) kann eine primitive Gruppe, welche die alternierende Gruppe nicht in sich schliesst, keine Cirkularsubstitution eines Primzahlgrades enthalten, welcher geringer ist als $\frac{2n}{3}$. Bedeutet p eine beliebige Primzahl, welche kleiner ist als $\frac{2n}{3}$ und p^f die höchste Potenz von p, welche in $n!$ aufgeht, so ist die Ordnung einer primitiven Gruppe G nicht durch p^f teilbar. Denn sonst umschlösse G eine Untergruppe, welche der Gruppe des Grades n und der Ordnung p^f ähnlich wäre; diese aber enthält nach der Konstruktion eine Cirkularsubstitution des Grades p, und das müsste demnach mit G gleichfalls der Fall sein. Daher enthält $\varrho=n!:r$ den Faktor p mindestens einmal.

Was von p bewiesen ist, gilt für jede Primzahl, die $<\frac{2n}{3}$ ist, und also auch für ihr Produkt. Daher folgt:

Lehrsatz V. Ist die Gruppe einer Funktion, welche mehr als zwei Werte besitzt, primitiv, so ist die Anzahl der Werte dieser Funktion ein Vielfaches des Produktes aller Primzahlen, welche kleiner als $\frac{2n}{3}$ sind.

---

* Cauchy: Journ. de l'Ecole Polytechn. X Cahier; Bertrand: ibid. XXX Cahier; Abel: Oeuvres complètes I. p. 13—21; J. A. Serret: Journ. de l'Ecole Polytechn. XXXII Cahier; C. Jordan: Traité etc. p. 67—75.

** C. Jordan: Traité etc. p. 664. Note C.

§ 116. Mit Hilfe dieses Satzes können wir Folgendes zeigen:

Lehrsatz VI. Es bedeute k irgend eine konstante Zahl. Die Funktionen von n Elementen, welche in Beziehung auf $n-k$ derselben alternierend oder symmetrisch sind, haben weniger Werte als diejenigen, welche es nicht sind. Für kleine Werte von n lässt der Satz Ausnahmen zu; oberhalb einer gewissen, von k abhängigen Grenze für n ist er stets richtig.*

Ist φ eine in $n-k$ Elementen alternierende Funktion, so ist die Ordnung der zugehörigen Gruppe ein Vielfaches von $\frac{1}{2}(n-k)!$, die Anzahl ϱ der Werte dieser Funktion daher höchstens gleich

$$\text{A)} \qquad 2 \cdot n(n-1)(n-2) \ldots (n-k+1).$$

Ist ψ eine Funktion, welche weder alternierend noch symmetrisch in $n-k$ Elementen ist, so kann sie entweder in Beziehung auf weniger als auf $n-k$ Elemente transitiv sein, oder in Beziehung auf $n-\varkappa$ $(\varkappa \leqq k)$; nur darf im letzteren Falle ψ nicht auch symmetrisch oder alternierend in den $n-\varkappa$ transitiv verbundenen Elementen werden.

Wir suchen für beide Fälle ein Minimum der Wertezahl von ψ und werden dabei zeigen, dass es für hinreichend grosse n grösser ist, als das eben gefundene Maximum A) der Wertezahl von φ.

§ 117. Es sei zuerst ψ nach weniger als $n-k$ Elementen transitiv. Dann ist die Ordnung der zugehörigen Gruppe ein Teiler von

$$\lambda_1! \, \lambda_2! \, \lambda_3! \ldots, \quad \text{wenn} \quad \lambda_1 + \lambda_2 + \lambda_3 + \ldots = n, \ (\lambda_\alpha < n-k).$$

Dieses Produkt wird ein Maximum, wenn eins der λ so gross als möglich, nämlich gleich $n-k-1$, ein zweites so gross als möglich, nämlich gleich $k+1$ angenommen wird. Dabei ist also nur $k+1 < n-k$, $n > 2k+1$ vorausgesetzt. Das Maximum für die Ordnung der Gruppe ist infolgedessen

$$(n-k-1)! \, (k+1)!$$

und das Minimum für die Wertezahl von ψ

$$\text{B)} \qquad \frac{n!}{(n-k-1)! \, (k+1)!} = \frac{n(n-1)(n-2) \ldots (n-k)}{1 \cdot 2 \cdot 3 \ldots (k+1)}.$$

Man erkennt, dass dieses Minimum B) das Maximum A) übertrifft, sobald

$$n > k + 2(k+1)!$$

gesetzt wird. Dies ist sonach die Grenze, oberhalb deren im ersten Falle unser Theorem keine Ausnahme mehr aufweisen kann.

---

* C. Jordan: Traité etc. p. 67.

§ 118. Es sei ferner im zweiten Falle ψ nach $(n-\varkappa)$, $(\varkappa \leqq k)$ Elementen transitiv, aber nach diesen Elementen weder alternierend noch symmetrisch. Die Gruppe G von ψ ist intransitiv; die Substitutionen derselben sind also Produkte aus je zwei anderen, von denen die einen, welche $\sigma_1, \sigma_2, \ldots$ heissen mögen, nur die Elemente $x_1, x_2, \ldots x_{n-\varkappa}$ transitiv verbinden, während die anderen $\tau_1, \tau_2, \ldots$ nur die übrigen Elemente $x_{n-\varkappa+1}, \ldots x_n$ enthalten.

Die Substitutionen der Gruppe G von ψ haben dann die Produktform

$$\sigma_1\tau_1,\ \sigma_2\tau_2,\ \sigma_3\tau_3,\ \ldots,\ \sigma_\alpha\tau_\alpha,\ \ldots,\ \sigma_\beta\tau_\beta,\ \ldots$$

wobei ein und dasselbe σ mit mehreren verschiedenen τ verbunden vorkommen kann. Es ist ohne Schwierigkeit zu erkennen, dass jedes σ gleich oft auftritt, so dass die Ordnung der Gruppe G ein Vielfaches der Ordnung der Gruppe $\Sigma = [\sigma_1, \sigma_2, \ldots]$ wird.

Wir wollen zeigen, dass Σ weder alternierend noch symmetrisch sein kann, da sonst auch G alternierend oder symmetrisch in $(n-\varkappa)$ Elementen wäre, was der Voraussetzung nach nicht angeht. Wäre Σ alternierend, so hätte diese Gruppe die Ordnung $\frac{1}{2}(n-\varkappa)!$; dies übertrifft die Maximalzahl $\varkappa!$ der Ordnung von $T = [\tau_1, \tau_2, \ldots]$ von $\varkappa$ Elementen, sobald $n > 2k$ ist. Folglich giebt es in G Substitutionen $\sigma_\alpha\tau_\alpha$, $\sigma_\beta\tau_\beta$, in denen $\tau_\alpha = \tau_\beta$, aber $\sigma_\alpha \neq \sigma_\beta$ ist; demnach auch Substitutionen $\sigma_\alpha\tau_\alpha(\sigma_\beta\tau_\beta)^{-1} = \sigma_\alpha\sigma_\beta^{-1}$, welche nur die Elemente x_1, $x_2, \ldots x_{n-\varkappa}$ der ersten Art enthalten. Die Gesamtheit derselben bildet eine ausgezeichnete Untergruppe H von G; sie ändert sich nicht bei Transformationen von G noch auch bei solchen von Σ, da $\tau_\alpha, \tau_\beta, \ldots$ gar keinen Einfluss auf H ausüben können. H bildet also auch eine ausgezeichnete Untergruppe der alternierenden Gruppe Σ, d. h. sie fällt mit ihr zusammen (§ 84). $H = \Sigma$ ist demnach eine Untergruppe von G, und ψ wird gegen die Annahme in $(n-\varkappa)$ Elementen alternierend.

§ 119. Es ist daher das Maximum für die Ordnung der Gruppe G gleich dem Produkte aus $\varkappa!$ und der Maximalordnung einer nicht alternierenden, transitiven Gruppe von $(n-\varkappa)$ Elementen. Diese möge $R(n-\varkappa)$ heissen. Dann ist das Minimum für die Wertezahl von ψ

$$\text{C)} \qquad \frac{n!}{\varkappa!\, R(n-\varkappa)} = \frac{(n-\varkappa)!}{R(n-\varkappa)} \cdot \frac{n(n-1)\ldots(n-\varkappa+1)}{\varkappa!}.$$

Wir haben jetzt noch $R(n-\varkappa)$, die Maximalordnung einer transitiven, nicht alternierenden Gruppe von $(n-\varkappa)$ Elementen oder $\frac{(n-\varkappa)!}{R(n-\varkappa)}$, die Minimalzahl für die Werte einer transitiven, nicht alternierenden Funktion von $(n-\varkappa)$ Elementen zu bestimmen.

Ist diese Funktion der $(n-\varkappa)$ Elemente imprimitiv, so zeigt der Lehrsatz aus § 72, dass die Minimalzahl folgende wird:

$$C_1) \qquad \frac{(n-\varkappa)!}{2\{[\frac{1}{2}(n-\varkappa)]!\}^2} = \frac{1}{2}\frac{(n-\varkappa)(n-\varkappa-1)\ldots\left(\frac{n-\varkappa}{2}+1\right)}{[\frac{1}{2}(n-\varkappa)]!}.$$

Setzen wir dies in C) ein, so erhalten wir als Minimum für die Wertezahl von ψ

$$C'_1) \qquad \frac{1}{2}\frac{n(n-1)\ldots(n-\varkappa+1)(n-\varkappa)\ldots\left(\frac{n-\varkappa}{2}+1\right)}{\varkappa![\frac{1}{2}(n-\varkappa)]!}.$$

Diese Zahl vergleichen wir mit der Maximalzahl A) und untersuchen, ob über einer gewissen Grenze für n der Wert $C'_1)$ grösser wird als A), d. h. ob man erhält

$$n(n-1)\ldots(n-\varkappa+1).(n-\varkappa)\ldots\left(\frac{n-\varkappa}{2}+1\right)$$
$$> 4.\varkappa!\,\frac{n-\varkappa}{2}!\,n.(n-1)\ldots(n-k+1).$$

Bei wachsendem n wird $\frac{n-\varkappa}{2}+1 < n-k+1$; es ist also zu beweisen, dass

$$(n-k)(n-k-1)\ldots\left(\frac{n-\varkappa}{2}+1\right) > 4.\varkappa!\,\frac{n-\varkappa}{2}!$$

wird. Dies ist ersichtlich, sobald man die rechte Seite unter der Form schreibt

$$(4.\varkappa![k-\varkappa]!)\cdot\left(\left[\frac{n-\varkappa}{2}\right]\left[\frac{n-\varkappa}{2}-1\right]\ldots[k-\varkappa+1]\right).$$

Denn jetzt ist der erste Faktor für wachsende n konstant, und das Verhältnis der linken Seite zur zweiten Klammer der rechten Seite hat zur Grenze

$$2^{\frac{n+\varkappa}{2}-k}.$$

§ 120. Ist endlich die Funktion ψ der $(n-\varkappa)$ Elemente primitiv, so greifen wir auf den Hilfssatz von § 115 zurück. Es folgt aus ihm, dass die Minimalzahl der Werte von ψ das Produkt aus allen Primzahlen wird, welche kleiner als $\frac{2}{3}(n-\varkappa)$ sind. Wir wollen dieses Produkt durch

$$P\left[\frac{2(n-\varkappa)}{3}\right]$$

bezeichnen. Führen wir es in C) ein, so ergiebt sich

$$C_2) \qquad P\left[\frac{2(n-\varkappa)}{3}\right]\frac{n(n-1)\ldots(n-\varkappa+1)}{\varkappa!}.$$

Es muss nun auch hier gezeigt werden, dass für hinlänglich grosse n der Wert A) kleiner ist als C_2), oder dass

$$P\left[\frac{2\,(n-\varkappa)}{3}\right] > 2\,.\,\varkappa!\,(n-\varkappa)\,(n-\varkappa-1)\,\ldots\,(n-k+1)$$

wird. Die rechte Seite wird stark vermehrt, wenn wir statt jedes $n-\varkappa-\alpha$ den ersten Faktor $n-\varkappa$ einsetzen. Da $k-\varkappa$ derartige Faktoren vorhanden sind, so tritt dann $(n-\varkappa)^{k-\varkappa}$ auf; schreiben wir ν statt $\frac{2\,(n-\varkappa)}{3}$, also $\frac{3\nu}{2}$ statt $(n-\varkappa)$, so braucht nur bewiesen zu werden, dass die Ungleichheit gilt

$$P(\nu) > [2\,.\,(\tfrac{3}{2})^{k-\varkappa}\,.\,\varkappa!]\,\nu^{k-\varkappa},$$

wenn man ν wachsen lässt, oder dass

$$\frac{P(\nu)}{\nu^{k-\varkappa}} > [2\,.\,(\tfrac{3}{2})^{k-\varkappa}\,.\,\varkappa!]$$

wird.

Dies kann man entweder durch wirkliche Ausführung induktiv erkennen, oder auch durch Benutzung des Tchebichef'schen Satzes, dass zwischen ν und $2\nu-2$ stets eine Primzahl liegt, falls ν grösser ist als 3.

Man hat nämlich auf Grund dieses Theorems

$$P(2\nu) > \nu P(\nu),$$
$$(2\nu)^{k-\varkappa} = 2^{k-\varkappa}\,.\,\nu^{k-\varkappa},$$
$$\frac{P(2\nu)}{(2\nu)^{k-\varkappa}} > \frac{P(\nu)}{\nu^{k-\varkappa}} \cdot \frac{\nu}{2^{k-\varkappa}}.$$

Welchen Wert nun auch immer der erste Quotient auf der rechten Seite haben mag, man kann t stets so gross annehmen, dass die linke Seite in

$$\frac{P(2^t\nu)}{(2^t\nu)^{k-\varkappa}} > \frac{P(\nu)}{\nu^{k-\varkappa}} \cdot \left(\frac{\nu}{2^{k-\varkappa}}\right)^t$$

beliebig gross wird, falls man nur ν grösser angenommen hat als $2^{k-\varkappa}$. Damit ist dann also der Beweis unseres Satzes vollständig geliefert.

Natürlich sind die hierbei erlangten unteren Grenzen bei weitem zu hoch; in jedem besonderen Falle ist es möglich, dieselben zu vermindern. Da wir aber bereits die Speziallfälle bis für $\varrho = \frac{1}{2}n\,(n-1)$ behandelt haben, so ist es nicht angethan, auf diese Untersuchungen weiter einzugehen.

Siebentes Kapitel.

Untersuchung einiger besonderer Arten von Gruppen.

§ 121. Für unsere Untersuchungen ist es von Wichtigkeit, auf die Resultate von § 48 zurückzugreifen und einige Folgerungen daraus zu ziehen.*

Es sei $r = p^\alpha . m$ die Ordnung einer Gruppe G, p eine Primzahl, m relativ prim zu p. Wir sahen, dass G eine Gruppe H der Ordnung p^α enthält. J sei die Maximalgruppe aus G, welche mit H vertauschbar ist; J enthält H; seine Ordnung ist daher $p^\alpha . i$, wobei i ein Teiler von m und also prim zu p ist.

Ausser den Substitutionen von H enthält J keine, deren Ordnung p^β wäre. Ist t eine Substitution von J, welche H nicht angehört, so wird $\{H, t\}$ eine Gruppe, deren Ordnung gleich dem Produkte der Ordnung von H und dem Exponenten der niedrigsten Potenz von t ist, welche in H vorkommt (§ 37). Da $\{H, t\}$ in J enthalten ist, kann dieser Exponent nur ein Teiler von i, also die Ordnung von t, welche ein Vielfaches des Exponenten ist, keine Potenz von p sein.

Es ist $\frac{m}{i} = k \equiv 1 \pmod{p}$. Wir bilden die zu J gehörige Funktion χ und diejenigen $\frac{m}{i}$ Werte derselben, welche unter dem Einflusse von G entstehen:

$$\text{R)} \qquad \chi_1, \chi_2, \chi_3, \cdots \chi_k; \quad \left(k = \frac{m}{i}\right);$$

χ_γ möge aus χ_1 durch Anwendung einer Substitution σ_γ von G hervorgehen. Auf die Reihe R) wenden wir alle Substitutionen von H an. Bliebe bei allen z. B. χ_α ungeändert, so würde H zur Gruppe $\sigma_\alpha^{-1} J \sigma_\alpha$ von χ_α gehören. $\sigma_\alpha^{-1} J \sigma_\alpha$ enthält aber an Substitutionen der Ordnungen p^β nur diejenigen von $\sigma_\alpha^{-1} H \sigma_\alpha$, wie J nur die von H enthält. Es wäre also $\sigma_\alpha^{-1} H \sigma_\alpha = H$ zu setzen; dies widerspricht den Annahmen, denn σ_α kommt nicht in J vor, während alle Substitutionen, die mit H vertauschbar sind, in J auftreten sollen.

Durch die Substitutionen von H tritt daher χ_α mit einigen anderen χ in Verbindung. Die Anzahl der so transitiv verbundenen ist ein

* L. Sylow: Clebsch Ann. V. 584—594.

Teiler der Ordnung von H, also eine Potenz von p. Wir können somit $\chi_2, \chi_3, \ldots \chi_k$ in eine Anzahl von Systemen zusammenfassen, deren jedes eine Anzahl p^δ von Funktionen enthält. Folglich ist

$$k-1=p.\varkappa, \quad m=i(p\varkappa+1), \quad r=p^\alpha i(p\varkappa+1).$$

Alle Untergruppen von G, welche die Ordnung p^α haben, entstehen aus H durch Transformationen mit Substitutionen von G. Wir wenden alle Substitutionen einer solchen Gruppe H' der Ordnung p^α auf R) an; die $p\varkappa+1$ Werte dieser Reihe gruppieren sich dann zu einer neuen Anzahl von Systemen, deren jedes eine Anzahl $p^a, p^b, p^c, \ldots$ von Funktionen enthält. Daher ist

$$p\varkappa+1=p^a+p^b+p^c+\ldots$$

Diese Gleichung kann nur befriedigt sein, wenn mindestens einer der Exponenten $a, b, c, \ldots$ gleich 0 wird, d. h. wenn ein System nur eine Funktion χ enthält. Dies sei χ_β; dann ist $H'=\sigma_\beta^{-1}H\sigma_\beta$.

H' ist durch $p^\alpha.i$ Transformationen aus H ableitbar. Denn es ist

$$H'=\sigma_\beta^{-1}J^{-1}HJ\sigma_\beta=(J\sigma_\beta)^{-1}H(J\sigma_\beta),$$

also ist H' durch mindestens $p^\alpha.i$ Transformationen zu erhalten. Wenn ferner

$$H'=\tau^{-1}H\tau^{+1}=\sigma_\beta^{-1}H\sigma_\beta$$

ist, so wird

$$H=\sigma_\beta^{+1}\tau^{-1}H\tau\sigma_\beta^{-1}=(\tau\sigma_\beta^{-1})^{-1}H(\tau\sigma_\beta^{-1}).$$

$$\tau\sigma_\beta^{-1}=J, \quad \tau=J\sigma_\beta.$$

Es giebt demnach auch nur $p^\alpha i$ Transformationen dieser Art.

Hiermit ist bewiesen:

Lehrsatz I. Ist G eine Gruppe, deren Ordnung r durch p^α, aber durch keine höhere Potenz der Primzahl p teilbar ist, H eine der in G enthaltenen Gruppen der Ordnung p^α, J die allgemeinste mit H vertauschbare Untergruppe von G, deren Ordnung wir $p^\alpha.i$ nennen, so wird die Ordnung von G

$$r=p^\alpha i(\varkappa p+1).$$

Jede Untergruppe H' von G, welche die Ordnung p^α besitzt, ist eine Transformierte von H. Derartiger Gruppen giebt es $\varkappa p+1$, und jede ist durch $p^\alpha i$ Transformationen aus H ableitbar.

§ 122. Wir kamen bei der Besprechung des Isomorphismus auf transitive Gruppen, bei denen Grad- und Ordnungszahlen einander gleich waren. Es zeigten sich mehrere interessante Eigenschaften solcher Gruppen. Wir wollen solche Gruppen in den nächsten Paragraphen als Gruppen Ω bezeichnen.

Rechnet man alle einander einstufig isomorphen transitiven Gruppen, bei denen dann also die Ordnungszahlen r denselben Wert haben, zu einer Klasse von Gruppen, so enthält eine jede dieser Klassen einen und auch nur einen Typus einer Gruppe Ω (§ 90). Die Aufstellung aller Typen der Gruppen Ω des Grades und der Ordnung r liefert demnach die Repräsentanten aller zu r gehörigen Klassen und damit auch die Anzahl derselben. Diese Aufstellung ist von Wichtigkeit, da isomorphe Gruppen dieselben Faktoren der Zusammensetzung haben und diese bei der algebraischen Lösung von Gleichungen eine bedeutende Rolle spielen werden.

Einen Typus können wir ganz allgemein aufstellen. Er wird durch die Potenzen einer Cirkularsubstitution gebildet. Wir nennen eine solche Gruppe Ω ein cyklische Gruppe und jede Funktion von n Veränderlichen, welche unter dem Einflusse einer cyklischen Gruppe des Grades n ungeändert bleibt, eine cyklische Funktion.

Wir wollen uns jetzt auf die Betrachtung cyklischer Funktionen vom Primzahlgrade p beschränken. Es sei $s=(x_1 x_2 \ldots x_p)$, ω irgend eine primitive p^{te} Wurzel der Einheit und

$$\varphi=(x_1+\omega x_2+\omega^2 x_3+\ldots+\omega^{p-1}x_p)^p.$$

Dann ist φ eine zur Gruppe $G=[1, s, s^2, \ldots s^{p-1}]$ gehörige cyklische Funktion. Denn φ wird unter dem Einflusse von s^α zu

$$(x_{\alpha+1}+\omega x_{\alpha+2}+\ldots+x_\alpha\omega^{p-1})^p=\omega^{\alpha p}(x_{\alpha+1}+\omega x_{\alpha+2}+\ldots+\omega^{p-1}x_\alpha)^p$$
$$=(x_1+\omega x_2+\ldots+\omega^{p-1}x_p)^p=\varphi$$

und bleibt also für G ungeändert.

Wenn umgekehrt bei unabhängigen x_α für irgend eine Substitution t

$$\varphi_t=\varphi_1$$

und daher

$$\sqrt[p]{\varphi_t}=\omega^\beta\sqrt[p]{\varphi_1}$$

ist, so würde wegen der Unabhängigkeit der x von einander folgen, dass durch t

$$x_{\gamma+1}\omega^\gamma \quad \text{in} \quad x_{t_{\gamma+1}}\omega^\gamma\omega^\beta=x_{t_{\gamma+1}}\omega^{\beta+\gamma}$$

übergeht, und da φ den Summanden $x_{\beta+\gamma+1}\omega^{\beta+\gamma}$ enthält, muss für jedes γ

$$t_{\gamma+1}=\beta+\gamma+1; \quad x_{t_1}=x_{\beta+1}, \quad x_{t_2}=x_{\beta+2}, \ldots; \quad t=s^\beta$$

sein; also gehört φ zu G.

Es ist ersichtlich, dass für $r=p$ die Gruppen G den einzig möglichen Typus Ω liefern.

§ 123. Wir suchen jetzt alle Typen der Gruppen Ω vom Grade und der Ordnung $p.q$, wo p, q Primzahlen sind, die fürs erste von

einander verschieden angenommen sein sollen; p möge die grössere von beiden sein.

1) Ein Typus, derjenige einer cyklischen Gruppe, ist uns bereits bekannt. Er wird durch das Vorkommen einer Substitution der Ordnung $p.q$ charakterisiert.

2) Giebt es andere Typen, so kann in diesen keine Substitution der Ordnung pq vorkommen, weil dies auf 1) zurückführen würde; es sind also nur die Ordnungen p, q, 1 zu erwarten. Eine Substitution s der Ordnung p ist sicher vorhanden; sie und ihre Potenzen bilden in Ω eine Untergruppe H der Ordnung p; gäbe es noch andere derartige Untergruppen H', so würde die Anzahl derselben $\varkappa p+1$ sein, wo $\varkappa > 0$ wäre; alle diese hätten eine und nur eine Substitution gemeinsam, nämlich die Einheit; folglich enthielten sie zusammen

$$(p-1)(p\varkappa+1)+1 = p[(p-1)\varkappa-1] \geq p.q$$

Substitutionen; das geht nicht an, also ist $\varkappa = 0$. Nun liefert H nur p Substitutionen; die übrigen sind sämtlich von der Ordnung q; ihre Anzahl ist

$$pq-p = (q-1)p;$$

also giebt es p Untergruppen der Ordnung q, und nach dem Lehrsatze I) muss demnach

$$p = q\lambda+1, \quad \lambda = \frac{p-1}{q},$$

also q ein Teiler von $p-1$ sein. Nur in diesem Falle sind neue Typen Ω möglich.

3) Alle Substitutionen der Ordnung q müssen die Gruppe H der Ordnung p in sich selbst transformieren. Dies kann so geschehen, dass eine Substitution t der Ordnung q dabei eine Substitution s der Ordnung p in sich selbst umwandelt. Es sei diese letztere

$$s = (x_1^1 x_2^1 \dots x_p^1)(x_1^2 x_2^2 \dots x_p^2) \dots (x_1^q x_2^q \dots x_p^q).$$

Nun dürfen in keinem Cyklus von t zwei Elemente mit gleichem oberen Index vorkommen. Denn eine passende Potenz von t würde diese aufeinander folgen lassen, und diese Potenz gäbe durch Multiplikation mit einer Potenz von s eine Substitution, welche, ohne dass sie sich auf die Einheit reduzierte, weniger als $p.q$ Elemente enthielte.

Wir können folglich einen der Cyklen von t gleich

$$(x_1^1 x_1^2 x_1^3 \dots x_1^q)$$

setzen, was ja stets durch geeignete Bezeichnung der Elemente oder der unteren Indices zu erreichen ist. Dann erkennt man aus

dass t auf
$$t^{-1}st = s,$$
x_2^{α} folgen lässt $x_2^{\alpha+1}$, auf x_3^{α} ebenso $x_3^{\alpha+1}$, ...,
so dass wir erhalten, wenn die oberen Indices mod. q reduziert werden,
$$t = (x_1^{\,1}x_1^{\,2}x_1^{\,3}\dots x_1^{\,q})(x_2^{\,1}x_2^{\,2}\dots x_2^{\,q})\dots(x_p^{\,1}x_p^{\,2}\dots x_p^{\,q}),$$
$$st = (x_1^{\,1}x_2^{\,2}\dots x_q^{\,q}x_{q+1}^{\,1}x_{q+2}^{\,2}\dots x_p^{\,\pi}x_1^{\,\pi+1}\dots)\dots$$
Hier muss jeder obere dem unteren Iedex mod. q kongruent, also auch
$$p \equiv \pi \pmod{q}$$
sein, und damit der Cyklus mit dem Elemente $x_p^{\,\pi}$ sich schliesst, müsste
$$\pi + 1 \equiv p + 1 \equiv 1 \pmod{q}$$
sein, was nicht möglich ist. st enthält also alle $p.q$ Elemente in einem Cyklus. Wir kommen daher bei der Annahme $t^{-1}st = s$ zum Typus 1) der cyklischen Gruppen zurück.

4) Alle Substitutionen der Ordnung q müssen die Gruppe H der Ordnung p in sich selbst transformieren. Dies kann zweitens so geschehen, dass eine Substitution t der Ordnung q dabei eine Substitution s der Ordnung p in s^{α} transformiert. Es sei
$$s = (x_1^{\,1}x_2^{\,1}\dots x_p^{\,1})(x_1^{\,2}x_2^{\,2}\dots x_p^{\,2})\dots(x_1^{\,q}x_2^{\,q}\dots x_p^{\,q}).$$
Wir können aus denselben Gründen wie oben einen Cyklus von t gleich
$$(x_1^{\,1}x_1^{\,2}x_1^{\,3}\dots x_1^{\,q})$$
setzen. Dann erkennt man aus
$$t^{-1}st = s^{\alpha},$$
dass t auf
$x_2^{\,\beta}$ folgen lässt $x_{\alpha+1}^{\,\beta+1}$, auf $x_3^{\,\beta}$ ebenso $x_{2\alpha+1}^{\,\beta+1}$,
auf $x_{\alpha+1}^{\,\beta}$ ebenso $x_{\alpha\alpha+1}^{\,\beta+1}$, ...,
so dass wir erhalten
$$t = (x_1^{\,1}x_1^{\,2}\dots x_1^{\,q})\dots(x_{\alpha+1}^{\,1}x_{\alpha\alpha+1}^{\,2}x_{\alpha\alpha^2+1}^{\,3}\dots x_{\alpha\alpha^{q-1}+1}^{\,q}\dots)\dots$$
Soll der angedeutete Cyklus mit jenem letzten Gliede $x_{\alpha\alpha^{q-1}+1}^{\,q}$ geschlossen sein, so ist
$$\alpha\alpha^q + 1 \equiv \alpha + 1 \pmod{p}, \quad \alpha^q \equiv 1 \pmod{p}$$
zu setzen. Hieraus ersehen wir zuerst, dass q ein Teiler von $p-1$ ist, was wir schon oben fanden; ferner, dass α zum Exponenten q gehören muss und dass es also $q-1$ Werte $\alpha_1, \alpha_2, \dots \alpha_{q-1}$ für α giebt; endlich, dass alle diese den Potenzen eines beliebigen unter ihnen mod. p kongruent sind. Aus $t^{-1}st = s^{\alpha}$ folgt
$$t^{-2}st^2 = s^{\alpha^2}, \quad t^{-3}st^3 = s^{\alpha^3}, \dots;$$
kommt also die Umwandlung von s durch Transformation mit t in eine beliebige Potenz mit dem Exponenten α_λ vor, so giebt es auch

Substitutionen, welche s in die Potenz a_1, a_2, ... a_{q-1} von s umwandeln. Demnach wird die Wahl von a_λ ohne Einfluss auf den Typus der Gruppe sein, und es giebt, wenn überhaupt einen, so auch nur einen Typus, der aus s und t gebildet ist.

Die Potenzen von t, nämlich t^1, t^2, ... t^{q-1}, liefern $(q-1)$ verschiedene Substitutionen der Ordnung q; ferner werden die $(q-1)$ ersten Potenzen aller

$$s^{-\beta+1}.t.s^{\beta-1} = (x_\beta{}^1 x_\beta{}^2 \dots x_\beta{}^q) \dots \quad (\beta = 2, 3, \dots p)$$

in Ω vorkommen. Dies giebt zusammen $p.(q-1)$ Substitutionen der Ordnung q; die Gruppe H der Ordnung p enthält p Substitutionen, und so hat man wirklich alle $p.q$ Substitutionen, unter denen keine von der Ordnung $p.q$ ist.

Hier haben wir also einen neuen Typus erlangt.

§ 124. Endlich sind noch alle Typen der Gruppen Ω vom Grade p^2 aufzusuchen.

1) Ein Typus, derjenige der cyklischen Gruppe, ist uns bereits bekannt. Er wird durch das Vorkommen einer Substitution der Ordnung p^2 charakterisiert.

2) Giebt es andere Typen, so kann in diesen keine Substitution der Ordnung p^2 vorkommen; es sind folglich nur p^2-1 Substitutionen der Ordnung p und eine der Ordnung 1 zuzulassen. Es sei s eine der Substitutionen von Ω, t eine andere, nicht als Potenz von s darstellbare, dann wird Ω durch s und t bestimmt sein. Denn, da erst die p^{te} Potenz von t durch s ausdrückbar ist, so sind alle

$$s^a t^b \quad (a = 0, 1, \dots p-1; \quad b = 0, 1, \dots p-1)$$

von einander verschieden; folglich ist

$$\Omega = [s^a . t^b] \quad (a, b = 0, 1, \dots p-1),$$

und man hat die Beziehungsreihe

$$S) \qquad ts = s^{\delta_1} t^{\varepsilon_1}, \quad t^2 s = s^{\delta_2} t^{\varepsilon_2}, \dots t^{p-1} s = s^{\delta_{p-1}} t^{\varepsilon_{p-1}}.$$

Werden zwei der Exponenten δ einander gleich, so ersieht man aus

$$t^a s = s^\delta t^\varepsilon, \quad t^b s = s^\delta t^{\varepsilon'} \quad (a \neq b, \quad \varepsilon \neq \varepsilon'),$$

dass

$$(t^a s)^{-1} . (t^b s) = s^{-1} t^c s = (s^\delta t^\varepsilon)^{-1} (s^\delta t^{\varepsilon'}) = t^\gamma.$$

Da man statt t^c auch t setzen kann, so folgt, dass es in Ω ein t giebt, welches, durch s transformiert, sich in eine Potenz t^η von t umwandelt.

Dasselbe findet statt, wenn in der Reihe S) alle Exponenten δ von einander verschieden sind; denn einer von ihnen wird dann gleich 1 werden, da keiner gleich Null sein kann, und aus

$$t^a s = s t^\varepsilon \quad \text{folgt} \quad s^{-1} t^a s = t^\varepsilon.$$

3) Wir können also voraussetzen, dass eine Substitution

$$t = (x_1^{\,1} x_2^{\,1} \dots x_p^{\,1})(x_1^{\,2} x_2^{\,2} \dots x_p^{\,2}) \dots (x_1^{\,p} x_2^{\,p} \dots x_p^{\,p})$$

durch die Transformation mit s in eine Potenz t^η übergeführt wird. Den ersten Cyklus von s dürfen wir setzen, wie dies schon im vorigen Paragraphen geschah,

$$(x_1^{\,1} x_1^{\,2} x_1^{\,3} \dots x_1^{\,p}).$$

Ist $\eta = 1$, so ergiebt sich

$$\begin{aligned} s &= (x_1^{\,1} x_1^{\,2} \dots x_1^{\,p})(x_2^{\,1} x_2^{\,2} \dots x_2^{\,p}) \dots (x_p^{\,1} x_p^{\,2} \dots x_p^{\,p}), \\ st &= (x_1^{\,1} x_2^{\,2} x_3^{\,3} \dots)(x_1^{\,2} x_2^{\,3} x_3^{\,4} \dots) \dots \\ st^2 &= (x_1^{\,1} x_3^{\,2} x_5^{\,3} \dots)(x_1^{\,2} x_3^{\,3} x_5^{\,3} \dots) \dots \\ &\dots\dots\dots\dots\dots\dots \end{aligned}$$

Man erhält also die $p+1$ Substitutionen

$$s,\ t,\ st,\ st^2,\ \dots\ st^{p-1},$$

deren $(p-1)$ erste Potenzen nebst der identischen Substitution 1 die Gruppe Ω vollständig bestimmen.

4) Es könnte endlich

$$s^{-1} t s = t^a \quad (a \not\equiv 1)$$

sein. Dann wäre

$$s = (x_1^{\,1} x_1^{\,2} \dots x_1^{\,p})(x_2^{\,1} x_{a+1}^{\,2} x_{a^2+1}^{\,3} \dots x_{a^{p-1}+1}^{\,p} x_{a^p+1}^{\,1} \dots) \dots;$$

damit der zweite Cyklus nach den ersten p Elementen sich schliesst, muss sein

$$a^p + 1 \equiv 2, \quad a^p \equiv 1 \pmod{p};$$

das ist aber für $a \not\equiv 1$ unmöglich.

Stellen wir die bisherigen Resultate zusammen, so folgt:

Lehrsatz II. Es giebt drei Typen von Gruppen Ω, deren Grad und Ordnung gleich dem Produkte zweier Primzahlen ist; der eine Typus ist derjenige der cyklischen Gruppen.

---

§ 125. Wir betrachten jetzt eine andere Kategorie von Gruppen, solche nämlich, deren Substitutionen entweder kein oder nur ein oder alle Elemente ungeändert lassen. Den Grad der Gruppen nehmen wir gleich der Primzahl p.

Dann ist jede vorkommende Substitution regulär; denn enthielte sie nicht in allen ihren Cyklen gleich viele Elemente, so würden in einer geeigneten Potenz zwei oder mehrere Elemente zum

Wegfall gebracht werden können, ohne dass die Potenz gleich der Einheit würde.

Die Substitutionen, welche alle Elemente umsetzen, sind cyklisch; denn p ist eine Primzahl. Daraus folgt weiter: Die Gruppen sind transitiv; ferner nach § 90: die Anzahl der Substitutionen, welche alle Elemente umsetzen, ist gleich $p-1$. Wir können also

$$s = (x_1 x_2 x_3 \dots x_p)$$

nebst den ersten $p-1$ Potenzen als in den gesuchten Gruppen vorkommend annehmen.

Es handelt sich daher nur um die Bestimmung derjenigen Substitutionen, welche $p-1$ Elemente umsetzen. Es sei t irgend eine unter ihnen und

$$t^{-1}st$$

die Transformierte von s durch t; da diese der ursprünglichen Substitution ähnlich ist und also, wie diese, alle p Elemente enthält, so wird es eine Potenz von s

$$t^{-1}st = s^m = (x_1 x_{1+m} x_{1+2m} \dots);$$

hier muss natürlich statt eines jeden Index sein kleinster positiver Rest mod. p genommen werden. Da es lediglich von der Benennung abhängt, welches der Elemente von t nicht umgesetzt wird, so können wir annehmen, es sei x_1. Dann wird

$$t = (x_2 x_{m+1} x_{m^2+1} x_{m^3+1} \dots) \dots (x_{a+2} x_{am+1} x_{am^2+1} \dots) \dots$$

Es möge nun g eine primitive Wurzel (mod. p) sein, dann sind alle Reste der ersten $(p-1)$ Potenzen von g

$$\text{G)} \qquad g^1, g^2, g^3, \dots g^{p-2}, g^{p-1} \equiv 1 \pmod{p}$$

von einander verschieden, und wir können daher setzen

$$m \equiv g^\mu \pmod{p}.$$

Wir bezeichnen nun t durch t_μ; dann erkennt man, dass t_μ aus μ Cyklen von je $\frac{p-1}{\mu}$ Elementen besteht; denn jeder der Cyklen von t_μ schliesst sich, sobald

$$\begin{aligned} am^z + 1 &\equiv a+1, \\ m^z &\equiv g^{\mu z} \equiv 1 \end{aligned} \pmod{p}$$

wird; dies geschieht erst bei $z = \frac{p-1}{\mu}$.

Besteht ferner eine Substitution t_ν, welche x_1 ungeändert lässt, und welche ein jedes Element x_{a+1} durch $x_{a.g^\nu+1}$ ersetzt, dann ersetzt $t_\mu^\alpha t_\nu^\beta$ jedes

$$x_{a+1} \quad \text{durch} \quad x_{a.g^{\alpha\mu+\beta\nu}+1}.$$

Bestimmen wir jetzt α, β so, dass $\alpha\mu+\beta\nu$ dem kleinsten gemeinsamen Teiler ω von μ, ν (mod. p) kongruent wird, so erhalten wir

$$t_\omega = t_\mu^{\alpha} t_\nu^{\beta},$$

wobei dann t_μ und t_ν Potenzen von t_ω werden. So kann man fortfahren, bis alle Substitutionen, welche x_1 ungeändert lassen, als Potenzen einer unter ihnen t_σ und zwar derjenigen dargestellt sind, bei welcher g^σ die niedrigste in der Reihe G) vorkommende Potenz ist, welcher eine Substitution t entspricht.

Mit t_σ kommen alle $\frac{p-1}{\sigma}$ Potenzen von t_σ in unserer Gruppe vor. Dieselbe ist durch s und t_σ bestimmt und enthält nach § 62 $\frac{p(p-1)}{\sigma}$ Substitutionen. σ kann unter den Teilern von $p-1$ willkürlich gewählt werden.

§ 126. Um eine zu der eben konstruierten Gruppe gehörige Funktion aufzustellen, bilden wir zuerst die zu s gehörige cyklische Funktion

$$\psi_1 = (x_1 + \omega x_2 + \omega^2 x_3 + \ldots + \omega^{p-1} x_p)^p,$$

in der ω eine primitive p^{te} Einheitswurzel bedeutet. Auf ψ_1 wenden wir die Potenzen von t_σ an und erhalten

$$\psi_2 = (x_1 + \omega x_{g^\sigma+1} + \omega^2 x_{2g^\sigma+1} + \ldots + \omega^{p-1} x_{(p-1)g^\sigma+1})^p$$
$$\psi_3 = (x_1 + \omega x_{g^{2\sigma}+1} + \omega^2 x_{2g^{2\sigma}+1} + \ldots + \omega^{p-1} x_{(p-1)g^{2\sigma}+1})^p$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Alle ψ gehören als cyklische Funktionen zu der aus s gebildeten Gruppe; für die Substitution t_σ und deren Potenzen gehen sie in einander über; jede symmetrische Funktion von

$$\psi_1, \psi_2, \ldots \underbrace{\psi_{p-1}}_{\sigma}$$

wird also für alle Substitutionen der Form $s^a t_\sigma^b$ ungeändert bleiben; wählt man unter Einführung einer unbestimmten Grösse ψ

$$\Psi_\sigma = (\psi - \psi_1)(\psi - \psi_2)\ldots\underbrace{(\psi - \psi_{p-1})}_{\sigma},$$

so wird Ψ_σ umgekehrt auch nur für diese Substitutionen seinen Wert beibehalten. Ψ_σ gehört also zur oben gefundenen Gruppe.

§ 127. Setzen wir $\sigma = 1$, so wird die Ordnung der Gruppe $p.(p-1)$. Es nimmt t die Form an

$$t_1 = (x_2 x_{g+1} x_{g^2+1} \ldots x_{g^{p-2}+1});$$

die Gruppe wird also zweifach transitiv. Wir nennen sie die metacyklische Gruppe und die zugehörige Funktion Ψ_1 eine metacyklische Funktion.

Setzen wir $\sigma = 2$, so wird die Ordnung der Gruppe $p\frac{p-1}{2}$. Es nimmt t die Form an

$$t_2 = (x_2 x_{g^2+1} x_{g^4+1} \ldots)(x_{a+1} x_{ag^2+1} x_{ag^4+1} \ldots).$$

Die um 1 verminderten Indices in der ersten Klammer sind die quadratischen Reste mod. p; a ist ein beliebiger quadratischer Nichtrest mod. p Diese Gruppe heisst die halb-metacyklische Gruppe und eine zugehörige Funktion Ψ_τ eine halb-metacyklische Funktion.*

§ 128. Wir können alle Substitutionen der Gruppen Ω vom Primzahlgrade p, und ebenso diejenigen der in den letzten beiden Paragraphen behandelten Gruppen in einfacher Weise durch die Angabe der Indicesänderungen von $x_1, x_2, \ldots x_p$ darstellen. Die Substitutionen von Ω sind dann durch

$$s_\alpha = |z \quad z+\alpha| \pmod{p} \quad (\alpha = 0, 1, 2, \ldots p-1)$$

bestimmt; wir verstehen das Symbol, welches soeben eingeführt wurde, so, dass in der Substitution s_α jedes Element x_z durch $x_{z+\alpha}$ zu ersetzen, und statt $z+\alpha$ sein kleinster nicht negativer Rest (mod. p) einzuführen ist.

Die in den vorigen Paragraphen behandelten Gruppen enthalten dann erstens alle Substitutionen s_α, ferner aber auch, wenn wir daselbst alle Indices um 1 vermindert denken, diejenigen Substitutionen, bei denen jedes Index mit demselben Faktor multipliziert wird, also für $z = 0, 1, 2, \ldots p-1$,

$$\sigma_\beta = |z \quad \beta z| \pmod{p} \quad (\beta = 1, 2, 3, \ldots p-1).$$

In dem Ausdrucke der Substitutionen

$$t = |z \quad \beta z+\alpha| \pmod{p} \quad (\alpha = 0, 1, \ldots p-1; \quad \beta = 1, 2, \ldots p-1)$$

sind alle Substitutionen s_α, σ_β und deren Kombinationen enthalten. Da

$$|z \quad \beta z+\alpha| \,.\, |z \quad \beta_1 z+\alpha_1| = |z \quad \beta\beta_1 z+\alpha_1\beta+\alpha|$$

ist, so folgt, dass die t eine Gruppe des Grades p und der Ordnung $p(p-1)$ bilden; diese Gruppe stimmt daher mit der von uns in § 127 behandelten überein.

Setzt man fest, dass für β nur die Werte

$$\beta = g^{1\sigma}, g^{2\sigma}, g^{3\sigma}, \ldots g^{\frac{p-1}{\sigma}\sigma}$$

genommen werden sollen, so wird $\beta\beta_1$ wieder zu derselben Reihe gehören, und man erhält die Gruppe des Grades p und der Ordnung $p\frac{p-1}{\sigma}$, welche oben besprochen wurde.

---

* L. Kronecker; vergl. F. Klein: Clebsch Ann. XV, 258.

§ 129. Die Betrachtung der linearen gebrochenen Substitutionen (mod. p) führt uns zu Gruppen des Grades $p+1$ und der Ordnung $(p+1)p(p-1)$. Die zu behandelnden Substitutionen haben die Form

$$u = \left| \begin{matrix} z \\ \dfrac{\alpha z+\beta}{\gamma z+\delta} \end{matrix} \right| \pmod{p};$$

dabei soll z die Werte $0, 1, 2, \ldots p-1, \infty$ annehmen; die Elemente der Gruppe sind daher $x_0, x_1, x_2, \ldots x_{p-1}, x_\infty$. Durch die Werte α, β, γ, δ wird u bestimmt, aber umgekehrt kann ein u durch verschiedene Annahmen von α, β, γ, δ gegeben werden; um dies zu vermeiden oder einzuschränken, benutzen wir die Differenz

D) $$\alpha\delta - \beta\gamma,$$

die Determinante von u. Ist sie positiv, so dividieren wir Zähler und Nenner von $\dfrac{\alpha z+\beta}{\gamma z+\delta}$ durch $\sqrt{\alpha\delta-\beta\gamma}$, ist sie negativ durch $\sqrt{\beta\gamma-\alpha\delta}$; dadurch erreichen wir es, dass für die neuen Koefficienten die Gleichung

D') $$\alpha\delta - \beta\gamma \equiv \pm 1 \pmod{p}$$

besteht. Wäre nun für verschiedene Systeme α, β, γ, δ, respektive α_1, β_1, γ_1, δ_1

$$\frac{\alpha z+\beta}{\gamma z+\delta} \equiv \frac{\alpha_1 z+\beta_1}{\gamma_1 z+\delta_1} \pmod{p},$$

so würde aus $z=0$, $z=\infty$, $z=-\dfrac{\beta}{\alpha}$, $z=-\dfrac{\delta}{\gamma}$ folgen, dass entweder

oder $$\begin{matrix} \alpha_1 \equiv \alpha, & \beta_1 \equiv \beta, & \gamma_1 \equiv \gamma, & \delta_1 \equiv \delta \\ \alpha_1 \equiv -\alpha, & \beta_1 \equiv -\beta, & \gamma_1 \equiv -\gamma, & \delta_1 \equiv -\delta \end{matrix} \pmod{p}$$

sein muss. Nehmen wir den Spielraum für α, β, γ, δ von 0 bis $p-1$, so können und werden je zwei verschiedene Systeme der Koefficienten die gleiche Substitution u geben.

Durch D') ist angenommen, dass $\alpha\delta-\beta\gamma$ von Null verschieden sei; diese Einschränkung ist notwendig, denn unser Symbol kann nur dann eine Substitution darstellen, wenn für verschiedene z nicht

$$\frac{\alpha z+\beta}{\gamma z+\delta} \equiv \frac{\alpha z_1+\beta}{\gamma z_1+\delta}$$

sein kann. Das wird durch die Annahme $\alpha\delta \neq \beta\gamma$ verhindert.

Ein Index z der Substitution u kann nur dann ungeändert bleiben, wenn

E) $$\gamma z^2 + (\delta-\alpha)z - \beta \equiv 0 \pmod{q}$$

ist. Dementsprechend giebt es vier Arten von Substitutionen u:

a) Bei der ersten sind beide Wurzeln von E) imaginär; dies geschieht, falls

$$\left(\frac{\alpha+\delta}{2}\right)^2 \mp 1 \quad (\text{wenn } \alpha\delta-\beta\gamma=\pm 1 \text{ ist})$$

quadratischer Nichtrest (mod. q) ist. Die Substitution setzt dann alle Elemente $x_0, x_1, x_2, \ldots x_{p-1}, x_\infty$ um.

b) Bei der zweiten Art von Substitutionen fallen beide Wurzeln von E) zusammen. Dies geschieht, falls

$$\left(\frac{\alpha+\delta}{2}\right)^2 \mp 1 \equiv 0 \pmod{p} \quad (\text{wenn } \alpha\delta-\beta\gamma\equiv\pm 1 \text{ ist})$$

wird. Die Substitution lässt dann ein Element ungeändert.

c) Bei der dritten Art von Substitutionen sind beide Wurzeln von E) reell und von einander verschieden. Dies geschieht, falls

$$\left(\frac{\alpha+\delta}{2}\right)^2 \mp 1 \quad (\text{wenn } \alpha\delta-\beta\gamma\equiv\pm 1 \text{ ist})$$

(mod. p) quadratischer Rest ist. Die Substitution lässt dann zwei Elemente ungeändert.

d) Bei der vierten Art von Substitutionen ist die Gleichung E) identisch erfüllt. Dies geschieht, falls

$$\gamma\equiv 0, \quad \beta\equiv 0, \quad \alpha\equiv\delta \pmod{p}$$

wird. Die Substitution lässt dann alle Elemente ungeändert.

Endlich bemerken wir noch, dass

$$\text{M)} \quad \left|z\ \frac{\alpha z+\beta}{\gamma z+\delta}\right| \cdot \left|z\ \frac{\alpha_1 z+\beta_1}{\gamma_1 z+\delta_1}\right| = \left|z\ \frac{(\alpha\alpha_1+\beta\gamma_1)z+(\alpha\beta_1+\beta\delta_1)}{(\gamma\alpha_1+\delta\gamma_1)z+(\gamma\beta_1+\delta\delta_1)}\right|,$$

$$\text{N)} \quad (\alpha\delta-\beta\gamma)(\alpha_1\delta_1-\beta_1\gamma_1) = (\alpha\alpha_1+\beta\gamma_1)(\gamma\beta_1+\delta\delta_1) - (\alpha\beta_1+\beta\delta_1)(\gamma\alpha_1+\gamma\delta_1)$$

ist. Jetzt sammeln wir die erhaltenen Resultate:

Wir wählen α nicht $\equiv 0$ (mod. p), β und γ beliebig; dann giebt es zu jedem der so erhaltenen $(p-1)p^2$ Systeme zwei Lösungen von D'), von denen aber je zwei nur eine Substitution u geben; also erhält man p^3-p^2 Substitutionen. Wir wählen $\alpha\equiv 0$ (mod. p.), δ beliebig; dann muss wegen D') β im Bereiche $1, 2, \ldots p-1$ gewählt werden und zu jedem der so erlangten Systeme α, δ, β giebt es gemäss D') zwei Werte von γ. Aber auch hier liefern je zwei Lösungen nur ein u; also erhält man $p(p-1)$ Substitutionen. Zusammen hat man demnach $p^3-p=(p+1)p(p-1)$ gebrochene lineare Substitutionen. Diese bilden wegen M) eine Gruppe. Greift man aus allen Substitutionen nur diejenigen heraus, welche dem oberen Zeichen in D') entsprechen,

so erhält man $\frac{(p+1)p(p-1)}{2}$ Substitutionen u. Diese bilden wegen M), N) auch eine Gruppe; sie heisst „die Gruppe der Modulargleichungen für p“.*

Die Gruppen enthalten nur Substitutionen, welche alle $p+1$, oder p, oder $p-1$, oder überhaupt kein Element umsetzen. Die Substitutionen, welche ein Element ungeändert lassen, bilden eine zweifach transitive Gruppe.

Lehrsatz III. Die linearen gebrochenen Substitutionen (mod. p) bilden eine Gruppe des Grades $p+1$ und der Ordnung $(p+1)p(p-1)$; diejenigen unter ihnen, deren Determinante quadratischer Rest (mod. p) ist, bilden eine Untergruppe der Ordnung $\frac{(p+1)p(p-1)}{2}$, die Gruppe der Modulargleichungen für p. Lässt eine Substitution dieser Gruppen mehr als zwei Elemente ungeändert, so reduziert sie sich auf die Einheit. Die erstere der beiden Gruppen ist dreifach transitiv.

§ 130. Wir geben endlich noch die Konstruktion einer Funktion, die zu der Gruppe der linearen gebrochenen Substitutionen gehört. Wir bilden zunächst nach den Angaben von § 126 eine Funktion Ψ_1 der p Veränderlichen $x_0, x_1, \ldots x_{p-1}$, welche für die Gruppe aller

$$t = |z \quad \beta z + \alpha| \quad (\text{mod. } p.) \quad (\alpha = 0, 1, \ldots p-1;\ \beta = 1, 2, \ldots p-1)$$

und nur für sie ungeändert bleibt. Diese Gruppe ist eine Untergruppe der Gruppe der gebrochenen linearen Substitutionen, aus der sie durch $\gamma = 0$ hervorgeht. Die Anzahl der Werte von Ψ_1, welche durch die u hervorgerufen werden, ist gleich $(p+1)$; es mögen diese Werte

$$\Psi_1, \Psi_2, \ldots \Psi_{p+1}$$

sein, so dass die Reihe der Ψ_α unter dem Einflusse dieser Gruppe der gebrochenen linearen Substitutionen sich bis auf ihre Folge reproduziert. Versteht man daher unter Ψ eine unbestimmte Grösse und bildet

$$\Sigma = (\Psi - \Psi_1)(\Psi - \Psi_2) \ldots (\Psi - \Psi_{p+1}),$$

so wird diese Funktion zur Gruppe gehören.

---

§ 131. Wir wollen uns jetzt noch mit solchen Gruppen beschäftigen, deren Substitutionen unter einander vertauschbar sind.

---

* Vergl. J. Gierster; Clebsch Ann. 18, p. 319.

Doch können wir hierbei eine allgemeinere Behandlung eintreten lassen, welche die erlangten Resultate vielfach verwendbar macht.*

Es seien θ', θ'', θ''', ... Elemente in endlicher Anzahl und so beschaffen, dass sich aus je zweien derselben mittels eines bestimmten Verfahrens ein drittes ableiten lässt. Demnach soll, wenn das Resultat dieses Verfahrens durch f angedeutet wird, für zwei beliebige Elemente θ', θ'', welche auch mit einander identisch sein können, ein θ''' existieren, welches gleich $f(\theta', \theta'')$ ist. Überdies soll

$$f(\theta', \theta'') = f(\theta'', \theta'),$$

$$f(\theta', f[\theta'', \theta''']) = f(f[\theta', \theta''], \theta'''),$$

und aber, sobald θ'' und θ''' von einander verschieden sind, auch

$$f(\theta', \theta'') \neq f(\theta', \theta''')$$

sein. Dies vorausgesetzt, kann die mit $f(\theta', \theta'')$ angedeutete Operation durch die Multiplikation der Elemente θ', θ'' ersetzt werden, wenn man dabei an Stelle der vollkommenen Gleichheit eine blosse Äquivalenz einführt. Macht man von dem üblichen Äquivalenzzeichen $\sim$ Gebrauch, so wird hiernach die Äquivalenz

$$\theta'\theta'' \sim \theta'''$$

durch die Gleichung

$$f(\theta', \theta'') = \theta'''$$

definiert. Da die Anzahl der Elemente θ, welche mit n bezeichnet werden möge, als endlich vorausgesetzt ist, so haben dieselben folgende Eigenschaften:

I) Unter den verschiedenen Potenzen eines Elementes θ giebt es stets solche, die der Einheit äquivalent sind. Die Exponenten aller dieser Potenzen sind ganze Vielfache eines derselben, zu welchem das betreffende θ gehört.

II) Gehört irgend ein θ zum Exponenten ν, so gehören auch zu jedem Teiler von ν gewisse Elemente θ.

III) Wenn die beiden Exponenten ϱ und σ, zu denen respektive die Elemente θ' und θ'' gehören, relative Primzahlen sind, so gehört das Produkt $\theta'\theta''$ zum Exponenten $\varrho\sigma$.

IV) Ist n_1 die kleinste Zahl, welche die sämtlichen Exponenten als Teiler enthält, zu denen die n Elemente θ gehören, so giebt es auch Elemente, welche zu n_1 selbst gehören.

Der hier mit n_1 bezeichnete Exponent ist der grösste von allen, zu denen die verschiedenen Elemente θ gehören; zugleich ist n_1 ein

* L. Kronecker: Monatsber. d. Akad. d. Wissensch. z. Berlin Dezemb. 1870 p. 881. Das Nachfolgende ist dieser Abhandlung grossenteils wörtlich entnommen.

ganzes Vielfaches von jedem dieser Exponenten, und es findet demnach für jedes beliebige θ die Äquivalenz $\theta^{n_1} \sim 1$ statt.

§ 132. Gehört θ_1 zum Exponenten n_1, so lässt sich der Begriff der Äquivalenz dahin erweitern, dass zwei Elemente θ' und θ'' als „relativ äquivalent" angesehen werden, wenn für irgend eine ganze Zahl k:

$$\theta' . \theta_1^k \sim \theta''$$

ist. Das Äquivalenzzeichen $\sim$ bleibe für den früheren engeren Begriff der Äquivalenz reserviert. Sondert man nun aus sämtlichen Elementen θ ein vollständiges System solcher aus, die untereinander nicht relativ äquivalent sind, so genügt auch dieses den für das System sämtlicher Elemente θ oben aufgestellten Bedingungen und besitzt daher auch alle daraus abgeleiteten Eigenschaften. Es existiert also namentlich eine der Zahl n_1 entsprechende Zahl n_2, welche so beschaffen ist, dass die n_2^{te} Potenz eines jeden θ dieses neuen Systems relativ äquivalent Eins, d. h. $\sim \theta_1^k$ ist, und es existieren ferner Elemente $\theta_{,,}$, für welche keine niedrigere als die n_2^{te} Potenz relativ äquivalent der Einheit wird. Da für jedes Element θ die Äquivalenz $\theta^{n_1} \sim 1$ stattfindet, und also a fortiori θ^{n_1} auch relativ äquivalent Eins ist, so muss nach I) die Zahl n_1 gleich n_2 oder ein Vielfaches von n_2 sein. Ist nun

$$\theta_{,,}^{n_2} \sim \theta_1^k,$$

und erhebt man die Ausdrücke auf beiden Seiten zur Potenz $\frac{n_1}{n_2}$, so erhält man, wenn $\frac{k}{n_2} = m$ gesetzt wird, die Äquivalenz

$$\theta_1^{m n_1} \sim 1,$$

aus welcher, da θ_1 zum Exponenten n_1 gehört, unmittelbar folgt, dass m ganz und also k ein Vielfaches von n_2 sein muss. Es giebt demnach ein Element θ_2, definiert durch die Äquivalenz

$$\theta_2 \theta_1^m \sim \theta_{,,} \quad \text{oder} \quad \theta_2 \sim \theta_{,,} \theta_1^{n_1 - m},$$

dessen n_2^{te} Potenz nicht nur relativ, d. h. im weiteren Sinne, sondern auch im engeren Sinne der Einheit äquivalent ist, und welches (im zweifachen Sinne des Wertes) zum Exponenten n_2 gehört, da ja die Gleichung besteht

$$\theta_2^{n_2} \sim \theta_{,,}^{n_2} \theta_1^{n_1 n_2 - m n_2} \sim \theta_1^k \theta_1^{n_1 n_2 - m n_2} \sim \theta_1^{n_1 n_2} \sim 1.$$

Indem man nunmehr je zwei Elemente θ', θ'' als relativ äquivalent ansieht, für welche:

$$\theta' \theta_1^h \theta_2^k \sim \theta''$$

ist, gelangt man zu einem dem Elemente θ_2 entsprechenden θ_3, welches zum Exponenten n_3 gehört, der gleich n_2 oder ein Teiler von n_2

ist u. s. f., und man erhält auf diese Weise ein Fundamentalsystem von Elementen $\theta_1, \theta_2, \theta_3, \ldots$, welches die Eigenschaft hat, dass der Ausdruck

$$\theta_1^{h_1}\theta_2^{h_2}\theta_3^{h_3}\ldots \quad (h_i = 1, 2, \ldots n_i)$$

im Sinne der Äquivalenz sämtliche Elemente θ und zwar jedes nur ein mal darstellt. Dabei sind die Zahlen $n_1, n_2, n_3, \ldots$, zu denen respektive $\theta_1, \theta_2, \theta_3, \ldots$ gehören, so beschaffen, dass jede derselben durch die folgende teilbar oder ihr gleich ist; das Produkt $n_1 . n_2 . n_3 \ldots$ ist gleich der mit n bezeichneten Anzahl sämtlicher Elemente θ, und diese Zahl n enthält demnach keine anderen Primfaktoren als diejenigen, welche bereits in der ersten Zahl n_1 enthalten sind.

§ 133. In unserem Falle müssen die Elemente θ durch Substitutionen ersetzt werden, die mit einander vertauschbar sind. n, die Anzahl der Elemente θ, geht in die Ordnung r der Gruppe über.

Wir haben demnach:

Lehrsatz IV. Sind die Substitutionen einer Gruppe untereinander vertauschbar, so giebt es ein Fundamentalsystem von Substitutionen $s_1, s_2, s_3, \ldots$, welches die Eigenschaft besitzt, dass der Ausdruck

$$s_1^{h_1}s_2^{h_2}s_3^{h_3}\ldots \quad (h_i = 1, 2, \ldots r_i)$$

sämtliche Substitutionen der Gruppe und zwar jede nur ein mal darstellt. Dabei sind die Zahlen $r_1, r_2, r_3, \ldots$ die Ordnungen von $s_1, s_2, s_3, \ldots$ und so beschaffen, dass jede derselben durch die folgende teilbar oder ihr gleich ist; das Produkt dieser Ordnungen $r_1 r_2 r_3 \ldots$ ist gleich der Ordnung r der Gruppe.

Die Zahl r_1 ist als die Maximalzahl unter den Ordnungen bestimmt. Die Substitution s_1 dagegen nicht; es könnte auch ein s'_1, welches zu r_1 gehört, an ihre Stelle treten. Je nachdem man dann von s_1 oder von s'_1 ausgeht, könnten sich auch die Werte $r_2, r_3, \ldots$ ändern. Wir werden zeigen, dass dies nicht der Fall ist.

Alle Substitutionen

$$s_\alpha^a s_\beta^b s_\gamma^c \ldots$$

mit festen Indices bilden eine Untergruppe. Dies ist eine ausgezeichnete Untergruppe; denn es ist

$$(s_1^\eta s_2^\vartheta s_3^\iota \ldots)^{-1} s_\alpha^a s_\beta^b s_\gamma^c \ldots (s_1^\eta s_2^\vartheta s_3^\iota \ldots) = s_\alpha^a s_\beta^b s_\gamma^c \ldots,$$

da alle Substitutionen unter einander vertauschbar sind. Stellt man nun die Gruppen

$$s_1^a s_2^b s_3^c \ldots, \quad s_2^b s_3^c \ldots, \quad s_3^c \ldots$$

auf, so werden die $r_1, r_2, r_3, \ldots$ die Faktoren der Zusammensetzung; sie sind also konstant.

Lehrsatz V. Die in der obigen Darstellung auftretenden Zahlen $r_1, r_2, r_3, \ldots$ sind für die Gruppe invariant.

Achtes Kapitel.

Analytische Darstellung der Substitutionen. Die lineare Gruppe.

§ 134. Wir kamen im letzten Kapitel zu einer neuen, vierten Darstellung der Substitutionen, welche darin bestand, dass der analytische Ausdruck angegeben wurde, demgemäss jeder Index der Reihe $x_1, x_2, x_3, \ldots$ durch die Substitution umgewandelt wird. Geht nämlich der Index z in x_z durch die Substitution in $\varphi(z)$, d. h. x_z in $x_{\varphi(z)}$ über, so ist die Substitution s durch die Schreibweise

$$s = \left| z \quad \varphi(z) \right|$$

vollkommen bestimmt. Für $\varphi(z)$ darf natürlich nicht jede Funktion genommen werden; es muss nämlich die Reihe

$$x_1, x_2, x_3, \ldots x_n \quad \text{in} \quad x_{\varphi(1)}, x_{\varphi(2)}, x_{\varphi(3)}, \ldots x_{\varphi(n)}$$

derart übergehen, dass die Indices $\varphi(1), \varphi(2), \ldots \varphi(n)$ bis auf die Reihenfolge mit $1, 2, 3, \ldots n$ übereinstimmen. Dagegen kann jede gegebene Substitution in die verlangte Form umgesetzt werden. Denn wenn

$$\varphi(1) = i_1, \quad \varphi(2) = i_2, \quad \ldots \varphi(n) = i_n$$

gefordert wird, so konstruieren wir, der Lagrange'schen Interpolationsformel gemäss, für

$$F(z) = (z-1)(z-2)\ldots(z-n)$$

die Funktion, welche den Bedingungen genügt, in der Form

$$\varphi(z) = i_1 \frac{F(z)}{F'(z)(z-1)} + i_2 \frac{F(z)}{F'(z)(z-2)} + \ldots + i_n \frac{F(z)}{F'(z)(z-n)}.$$

Sie steigt in z bis zum Grade $n-1$. Es ist klar, dass man der Forderung durch unendlich viele Formen für $\varphi(z)$ genügen kann.

§ 135. Ist n eine Primzahl p, so kann man einerseits eine Erweiterung dadurch eintreten lassen, dass man die Indices $1, 2, 3, \ldots p$ durch ein beliebiges vollständiges Restsystem (mod. p) ersetzt denkt, also auch Indices zulässt, welche den Wert p überschreiten; andrerseits

kann man jede Form von $\varphi(z)$ ohne Schwierigkeit bis auf den Grad $p-1$ erniedrigen, da ja $z^p \equiv z \pmod p$ für alle Werte 0, 1, 2, ... $p-1$ von z gilt.

Speziell wird $F(z) \equiv z^p - z$ werden und $F'(z) \equiv pz^{p-1} - 1 \equiv -1$.

In diesem Falle $n = p$ kann man durch das folgende Theorem die Funktionen $\varphi(z)$ charakterisieren, welche geeignet sind, eine Substitution analytisch auszudrücken, bei denen demnach die Werte $\varphi(0)$, $\varphi(1)$, ... $\varphi(p-1)$ ein vollständiges Restsystem ausmachen.

Lehrsatz I. Damit $|z \quad \varphi(z)|$ eine Substitution von p Elementen ausdrücke, ist es notwendig und hinreichend, dass $\varphi(z)$ und seine $p-2$ ersten Potenzen sich auf den $p-2^{\text{ten}}$ Grad reduzieren, nachdem man sie mittels $z^p \equiv z$ auf den $p-1^{\text{ten}}$ Grad gebracht und alle Vielfachen von p unterdrückt hat.*

Es sei $$\varphi(z) = A_0 + A_1 z + A_2 z^2 + \ldots + A_{p-1} z^{p-1}$$

eine beliebige ganze Funktion mod. p. Wir bilden

$$[\varphi(z)]^m \equiv A_0^{(m)} + A_1^{(m)} z + A_2^{(m)} z^2 + \ldots + A_{p-1}^{(m)} z^{p-1} \pmod p$$

und erhalten, da für ein jedes $\alpha < p-1$

$$0^\alpha + 1^\alpha + 2^\alpha + \ldots + (p-1)^\alpha \equiv 0 \pmod p$$

ist, den Wert der Summe

$$\text{S)} \quad [\varphi(0)]^m + [\varphi(1)]^m + \ldots + [\varphi(p-1)]^m \equiv (p-1) A_{p-1}^{(m)} \equiv -A_{p-1}^{(m)} \pmod p.$$

Wenn nun $\varphi(z)$ zur Darstellung einer Substitution geeignet ist, so dass $\varphi(0)$, $\varphi(1)$, ... $\varphi(p-1)$ ein vollständiges Restsystem (mod. p) ergeben, dann können wir schliessen, dass für $m < p-1$

$$A_{p-1}^{(m)} \equiv 0 \pmod p$$

wird. Dies beweist die Notwendigkeit der aufgestellten Bedingung.

Wenn umgekehrt diese letzte Gleichung für eine gewisse Funktion $\varphi(z)$ erfüllt ist, so ergiebt sich aus der Richtigkeit von S) für $m = 1, 2, \ldots (p-2)$ mittels der Formeln B_1) aus § 4

$$[z - \varphi(0)][z - \varphi(1)] \ldots [z - \varphi(p-1)] \equiv z^p - \alpha z \pmod p.$$

Da hieraus folgt, dass die Wurzeln von $z^p - \alpha z \equiv 0$ ganze Zahlen sind, so gilt für jede Wurzel die andere Kongruenz $z^p - z \equiv 0$, also gilt auch für jede $(\alpha - 1) z \equiv 0$. Diese Kongruenz ersten Grades muss für p Werte $\varphi(0)$, ..., $\varphi(p-1)$ befriedigt sein. Wäre α nicht gleich 1, so wären die Wurzeln gleich Null und die Kongruenz $(p-2)^{\text{ten}}$ Grades

---

* Hermite: Comptes rendus de l'Académie des Sciences 57.

$$\varphi(z) \equiv A_0 + A_1 z + \ldots + A_{p-2} z^{p-2} \equiv 0 \pmod{p}$$

hätte p von einander verschiedene Wurzeln $z = 0, 1, \ldots (p-1)$. Also ist

$$[z - \varphi(0)]\,[z - \varphi(1)] \ldots [z - \varphi(p-1)] \equiv z^p - z$$
$$\equiv z(z-1)(z-2) \ldots [z - (p-1)],$$

d. h. die Werte $\varphi(0)$, $\varphi(1)$, $\ldots$ $\varphi(p-1)$ stimmen mit den Werten $0, 1, \ldots, (p-1)$ überein. Dies zeigt, dass die aufgestellte Bedingung hinreichend dafür ist, dass durch $|z \quad \varphi(z)|$ eine Substitution dargestellt werden kann.

§ 136. Statt durch einen einzigen, können wir die der Substitution unterworfenen Elemente x auch durch mehrere Indices kennzeichnen. Bei p^2 Elementen wäre es z. B. möglich, die beiden Indices z, u in $x_{z,u}$ von 0 bis $(p-1)$ gehen zu lassen. Eine Substitution unter diesen p^2 Elementen könnte dann durch

$$s = |z, u \quad \varphi(z, u), \ \psi(z, u)|$$

bezeichnet werden, wobei $\varphi(z, u)$, $\psi(z, u)$ ähnlichen Bedingungen zu unterwerfen sind, wie sie in § 134 besprochen wurden.

Ist $n = p^k$, so können die Elemente durch

$$x_{z_1, z_2, \ldots z_k} \quad (z_i = 0, 1, 2, \ldots, p-1)$$

bezeichnet werden; die Substitution s wird dann

$$s = |z_1, z_2, \ldots z_k \quad \varphi_1(z_1, z_2, \ldots z_k), \ \varphi_2(z_1, z_2, \ldots z_k), \ldots \varphi_k(z_1, z_2, \ldots z_k)|,$$

wodurch angedeutet werden soll, dass der Index

$$z_i \quad \text{in} \quad \varphi_i(z_1, z_2, \ldots z_k)$$

umgesetzt werden muss. Die Funktionen φ_1, φ_2, $\ldots$ φ_k müssen der Beschränkung unterliegen, dass die p^k verschiedenen Systeme z_1, z_2, $\ldots z_k$ auch p^k verschiedene Systeme φ_1, φ_2, $\ldots$ φ_k hervorrufen.

Man könnte diese Darstellungsart auch auf den Fall erweitern, dass n mehrere von einander verschiedene Primzahlen als Faktoren enthält. Hierauf gehen wir jedoch nicht ein, da die Theorie sich kompliziert.

§ 137. Die einfachsten analytischen Ausdrücke für Substitutionen von $n = m^k$ Elementen erhalten wir durch die Substitutionen von der linearen Form

1) $$s_{\alpha_1, \alpha_2, \ldots \alpha_k} = |z_1, z_2, \ldots z_k \quad z_1 + \alpha_1, \ z_2 + \alpha_2, \ \ldots z_k + \alpha_k|.$$

Die α sind beliebige ganze Zahlen mod. m; sie können also auf m^k verschiedene Arten gewählt werden. Ebensoviele Substitutionen dieser Form giebt es. Da

2) $$s_{\alpha_1, \alpha_2, \ldots \alpha_k} \cdot s_{\beta_1, \beta_2, \ldots \beta_k} = s_{\alpha_1 + \beta_1, \ \alpha_2 + \beta_2, \ \alpha_k + \beta_k}$$

ist, so bilden diese arithmetischen Substitutionen* eine Gruppe der Ordnung und des Grades m^k. Diese Gruppe ist transitiv, da man die α so wählen kann, dass ein beliebiges Element $x_{z_1, \dots z_k}$ in ein beliebiges andere $x_{\zeta_1, \dots \zeta_k}$ übergeführt wird. Es muss dazu

$$\alpha_1 = \zeta_1 - z_1, \quad \alpha_2 = \zeta_2 - z_2, \dots \alpha_k = \zeta_k - z_k$$

genommen werden. Es giebt nur eine Substitution der Gruppe, welche dies leistet.

Damit eine der arithmetischen Substitutionen ein Element x ungeändert lasse, muss

$$\alpha_1 \equiv 0, \quad \alpha_2 \equiv 0, \dots \alpha_k \equiv 0 \pmod{m}$$

sein. Dann lässt die Substitution alle Elemente ungeändert und reduziert sich auf die Einheit. Die Gruppe gehört also zu den im vorigen Kapitel behandelten Gruppen Ω.

Durch mehrmalige Anwendung der Formel 2) kommt man zu

$$s_{\alpha_1, \alpha_2, \dots \alpha_k} = s_{1,0,\dots 0}{}^{\alpha_1} \cdot s_{0,1,\dots 0}{}^{\alpha_2} \dots s_{0,0,\dots 1}{}^{\alpha_k},$$

so dass wir die Gruppe durch

3) $$G = \{ s_{1,0,\dots 0},\ s_{0,1,\dots 0},\ \dots\ s_{0,0,\dots 1} \}$$

bezeichnen können. Die in die Klammer aufgenommenen Substitutionen sind untereinander vertauschbar. Dasselbe findet daher bei allen Substitutionen von G statt.

§ 138. Wir suchen die allgemeinste Form der Substitutionen

$$t = | z_1, z_2, \dots z_k \quad \varphi_1(z_1, \dots z_k),\ \varphi_2(z_1, \dots z_k),\ \dots\ \varphi_k(z_1, \dots z_k) |,$$

welche mit G vertauschbar sind, für welche daher die Gleichung

$$t^{-1} s_{\alpha_1, \dots} t = s_{\beta_1, \dots}$$

gilt. Es reicht natürlich aus, dass $s_{\alpha_1, \dots}$ der Reihe nach gleich den in 3) angegebenen Substitutionen genommen werde. Es wird $t^{-1} s_{1,0,\dots 0} t$ auf

$$\varphi_\lambda(z_1, z_2, \dots z_k) \quad \text{folgen lassen} \quad \varphi_\lambda(z_1 + 1, z_2, \dots z_k);$$

also muss für $\lambda = 1, 2, 3, \dots k$ die Beziehungsreihe statthaben:

$$\varphi_\lambda(z_1 + 1, z_2, \dots z_k) \equiv \varphi_\lambda(z_1, z_2, \dots z_k) + a_\lambda \pmod{m}.$$

Ebenso ergiebt sich für $s_{0,1,\dots 0}, \dots s_{0,0,\dots 1}$

$$\varphi_\lambda(z_1, z_2 + 1, \dots z_k) \equiv \varphi_\lambda(z_1, z_2, \dots z_k) + b_\lambda \pmod{m}$$

$$\dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots$$

$$\varphi_\lambda(z_1, z_2, \dots z_k + 1) \equiv \varphi_\lambda(z_1, z_2, \dots z_k) + c_\lambda \pmod{m}.$$

Setzt man nun $\varphi_\lambda(0, 0, 0, \dots 0) \equiv \delta_\lambda$, so folgt aus diesen Gleichungen bei weiterer Reduktion der Indices z auf der rechten Seite der Kon-

* Cauchy: Exercices III, p. 232.

gruenzen die Natur der φ_λ als linearer Funktionen der z mit den konstanten Gliedern δ_λ. Hieraus ist die Form der Funktionen φ ersichtlich: Es wird

$$\varphi_\lambda(z_1, z_2, \ldots z_k) = a_\lambda z_1 + b_\lambda z_2 + \ldots + c_\lambda z_k + \delta_\lambda,$$

und für t ergiebt sich

$$t = |\, z_1, z_2, \ldots z_k \quad a_1 z_1 + b_1 z_2 + \ldots + c_1 z_k + \delta_1,\ a_2 z_1 + b_2 z_2 + \ldots + c_2 z_k + \delta_2, \ldots |;$$

dass umgekehrt alle Substitutionen dieser Form die Gruppe G in sich selbst transformieren, ist leicht einzusehen, da t z. B.

$$s_{1,0,0,\ldots 0} \quad \text{in} \quad |\, a_1 z_1 + b_1 z_2 + \ldots + c_1 z_k + \delta_1, \ldots \\ a_1(z_1 + 1) + b_1 z_2 + \ldots + c_1 z_k + \delta_1, \ldots |,$$

d. h. in die arithmetische Substitution

$$|\, \xi_1, \xi_2, \ldots \xi_k \quad \xi_1 + a_1,\ \xi_2 + a_2, \ \ldots\ \xi_k + a_k \,| = s_{a_1, a_2, \ldots a_k}$$

transformiert.

Man kann t durch linksseitige Multiplikation mit

$$s_{\delta_1, \delta_2, \ldots \delta_k}{}^{-1} = s_{-\delta_1, -\delta_2, \ldots -\delta_k}$$

auf die Form

$$t' = |\, z_1, z_2, \ldots z_k \quad a_1 z_1 + b_1 z_2 + \ldots + c_1 z_k,\ a_2 z_1 + b_2 z_2 + \ldots + c_2 z_k, \ldots \\ \ldots,\ a_k z_1 + b_k z_2 + \ldots + c_k z_k \,|$$

bringen. Eine solche Substitution möge eine geometrische Substitution* heissen.

Wir gehen auf eine Untersuchung derselben ein. Bewiesen ist bereits:

Lehrsatz II. Alle geometrischen Substitutionen in ihrer Verbindung mit den arithmetischen, und nur diese sind mit der Gruppe der arithmetischen Substitutionen vertauschbar.

§ 139. Es handelt sich zuerst um die Entscheidung darüber, ob die Konstanten $a_\lambda, b_\lambda, \ldots c_\lambda$ beliebig angenommen werden können. Einer Beschränkung müssen sie sicher unterworfen werden, da $x_{z_1, z_2, \ldots z_k}$ nicht in dasselbe x umgewandelt werden darf, wie $x_{\zeta_1, \zeta_2, \ldots \zeta_k}$, sobald das System $z_1, z_2, \ldots z_k$ nicht in allen Gliedern der Reihe nach mit $\zeta_1, \zeta_2, \ldots \zeta_k$ übereinstimmt. Allgemeiner: wenn ein bestimmtes Wertesystem $\zeta_1, \zeta_2, \ldots \zeta_k$ gegeben ist, dann muss aus

$$a_1 z_1 + b_1 z_2 + \ldots + c_1 z_k \equiv \zeta_1, \quad a_2 z_1 + b_2 z_2 + \ldots + c_2 z_k \equiv \zeta_2, \ldots \pmod{m}$$

das System $z_1, z_2, \ldots z_k$ ohne Zweideutigkeit berechnet werden können. Wir suchen diese Beschränkung analytisch auszudrücken.

---

* Cauchy: a. a. O.

Es ist

$$4)\quad \begin{cases} t = \\ \left| z_1, z_2, \ldots z_k \quad a_1 z_1 + b_1 z_2 + \ldots + c_1 z_k,\ a_2 z_1 + b_2 z_2 + \ldots + c_2 z_k, \ldots \right| \pmod m \\ t^{-1} = \\ \left| a_1 z_1 + b_1 z_2 + \ldots + c_1 z_k,\ a_2 z_1 + b_2 z_2 + \ldots + c_2 z_k, \ldots \quad z_1, z_2, \ldots \right| \\ = \left| \xi_1, \xi_2, \ldots \xi_k \quad \frac{1}{\Delta}\left(\frac{\partial \Delta}{\partial a_1}\xi_1 + \frac{\partial \Delta}{\partial a_2}\xi_2 + \ldots + \frac{\partial \Delta}{\partial a_k}\xi_k\right), \cdots \right| \pmod m, \end{cases}$$

wenn Δ die Determinante

$$5)\quad \Delta = \begin{vmatrix} a_1, b_1, \ldots c_1 \\ a_2, b_2, \ldots c_2 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ a_k, b_k, \ldots c_k \end{vmatrix}$$

bedeutet.

Aus 4) folgt, dass der grösste gemeinsame Teiler τ_1 von m und Δ auch $\frac{\partial \Delta}{\partial a_1}, \frac{\partial \Delta}{\partial a_2}, \ldots \frac{\partial \Delta}{\partial a_k}$ teilt. Denn wenn dies nicht der Fall wäre, könnte man $\xi_1, \xi_2, \ldots \xi_k$ so bestimmen, dass

$$\frac{\partial \Delta}{\partial a_1}\xi_1 + \frac{\partial \Delta}{\partial a_2}\xi_2 + \ldots + \frac{\partial \Delta}{\partial a_k}\xi_k$$

gleich dem grössten gemeinsamen Teiler von $\frac{\partial \Delta}{\partial a_1}, \frac{\partial \Delta}{\partial a_2}, \cdots$ wird. Dann hätte der Ausdruck

$$6)\quad \frac{1}{\Delta}\left(\frac{\partial \Delta}{\partial a_1}\xi_1 + \frac{\partial \Delta}{\partial a_2} + \ldots + \frac{\partial \Delta}{\partial a_k}\xi_k\right) \pmod m$$

überhaupt keinen Sinn.

Umgekehrt folgt aus 4), dass der grösste gemeinsame Teiler τ_2, von m und $\frac{\partial \Delta}{\partial a_1}, \frac{\partial \Delta}{\partial a_2}, \cdots$ in Δ aufgehen muss; denn wäre dies nicht der Fall, so könnte man $\xi_1, \xi_2, \ldots \xi_k$ nicht so wählen, dass der Wert von 6) relativ prim zu m würde, was doch notwendig gefordert werden muss, damit t^{-1} eine Substitution sei.

Es ist also $\tau_1 = \tau_2$; wir nennen den gemeinsamen Wert τ und setzen

$$\Delta = \tau\delta, \quad m = \tau\mu; \quad \frac{\partial \Delta}{\partial a_\lambda} = \tau\alpha_\lambda, \quad \frac{\partial \Delta}{\partial b_\lambda} = \tau\beta_\lambda, \quad \ldots \frac{\partial \Delta}{\partial c_\lambda} = \tau\gamma_\lambda.$$

Dann wird

$$7)\quad t^{-1} = \left| \xi_1, \xi_2, \ldots \xi_k \quad \frac{1}{\delta}(\alpha_1\xi_1 + \alpha_2\xi_2 + \ldots + \alpha_k\xi_k), \right.$$
$$\left. \frac{1}{\delta}(\beta_1\xi_1 + \beta_2\xi_2 + \ldots), \ldots \right| \pmod m.$$

Ferner hat man

$$\Delta^{k-1} = (\tau\delta)^{k-1} = \tau^k \begin{vmatrix} \alpha_1, \beta_1, \dots \gamma_1 \\ \alpha_2, \beta_2, \dots \gamma_2 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \alpha_k, \beta_k, \dots \gamma_k \end{vmatrix} = \tau^k D,$$

$$\delta^{k-1} = \tau D.$$

Es ist also δ, weil es mit τ einen gemeinsamen Faktor hat, nicht prim zu m. Der grösste gemeinsame Teiler von m und δ umfasst jedenfalls alle in τ enthaltenen Primfaktoren; er möge τ' heissen. Dann knüpfen sich an 7) dieselben Schlüsse wie oben an 4). Es wird τ' auch der grösste gemeinsame Teiler von m und $\alpha_1, \alpha_2, \dots \alpha_k$. So ergiebt sich

$$8)\quad \begin{cases} \delta = \delta'\tau', \quad m = \mu'\tau'; \quad \alpha_\lambda = \alpha'_\lambda\tau', \quad \beta_\lambda = \beta'_\lambda\tau', \dots \gamma_\lambda = \gamma'_\lambda\tau', \\ t^{-1} = \left| \xi_1, \xi_2, \dots \xi_k \quad \dfrac{1}{\delta'}(\alpha'_1\xi_1 + \alpha'_2\xi_2 + \dots + \alpha'_k\xi_k), \right. \\ \qquad\qquad \left. \dfrac{1}{\delta'}(\beta'_1\xi_1 + \beta'_2\xi_2 + \dots) \dots \right| \quad (\text{mod. } m), \\ \Delta^{k-1} = (\tau\tau'\delta')^{k-1} = \tau^k\tau'^k \begin{vmatrix} \alpha'_1, \beta'_1, \dots \gamma'_1 \\ \alpha'_2, \beta'_2, \dots \gamma'_2 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \end{vmatrix} = \tau^k\tau'^k D', \\ \delta'^{k-1} = \tau\tau' D'. \end{cases}$$

Es hat also auch δ' noch einen gemeinsamen Teiler mit m, der von 1 verschieden ist, falls dies bei τ', und also, falls es bei τ der Fall ist; auch er umfasst alle in τ enthaltenen Primfaktoren.

Man kann in dieser Weise ohne Ende weiter schliessen; da aber Δ^{k-1} eine endliche Zahl ist, so geht dies nicht an, d. h. damit t eine Substitution ist, muss $\tau = 1$, d. h. Δ relativ prim zu m sein.

§ 140. Diese Bedingung ist auch hinreichend. Denn die Kongruenzen

$$a_1 z_1 + b_1 z_2 + \dots + c_1 z_k \equiv \xi_1, \quad a_2 z_1 + b_2 z_2 + \dots + c_2 z_k \equiv \xi_2, \dots \quad (\text{mod. } m)$$

führen auf

$$z_1\Delta \equiv \frac{\partial\Delta}{\partial a_1}\xi_1 + \frac{\partial\Delta}{\partial a_2}\xi_2 + \dots + \frac{\partial\Delta}{\partial a_k}\xi_k, \quad z_2\Delta \equiv \frac{\partial\Delta}{\partial b_1}\xi_1 + \frac{\partial\Delta}{\partial b_2}\xi_2 + \dots + \frac{\partial\Delta}{\partial b_k}\xi_k, \dots$$

und diese letzteren lassen, wenn Δ und m keinen gemeinsamen Teiler haben, eine und auch nur eine Lösung zu, wie man erkennt, wenn man $\dfrac{1}{\Delta} \equiv \varepsilon \pmod{m}$ setzt.

Lehrsatz III. Damit der Ausdruck

$$t = | z_1, z_2, \ldots z_k \quad a_1 z_1 + b_1 z_2 + \ldots + c_1 z_k, \; a_2 z_1 + b_2 z_2 + \ldots + c_2 z_k, \ldots | \; (\mathrm{mod.}\, m.)$$

eine (geometrische) Substitution bedeute, ist es notwendig und hinreichend, dass

$$\Delta = \begin{vmatrix} a_1, b_1, \ldots c_1 \\ a_2, b_2, \ldots c_2 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_k, b_k, \ldots c_k \end{vmatrix}$$

relativ prim zum Modul m sei.

§ 141. Hieraus ist es möglich, die Anzahl r der für den Modul m vorhandenen geometrischen Substitutionen zu bestimmen.

Es möge $[m, \varrho]$ die Anzahl der Lösungen der Aufgabe angeben, ϱ Zahlen zu bestimmen, welche kleiner als m und relativ prim zu m sind.

Es sei N die Anzahl derjenigen geometrischen Substitutionen 1, t_2, t_3, ..., welche den ersten Index z_1 ungeändert lassen, τ_2 eine Substitution, welche z_1 ersetzt durch $a_1 z_1 + b_1 z_2 + \ldots + c_1 z_k$, dann werden τ_2, $t_2\tau_2$, $t_3\tau_2$, ... alle Substitutionen sein, welche dies thun, und sie werden sämtlich von einander verschieden sein. Ersetzt τ_3 den Index z_1 durch $a'_1 z_1 + b'_1 z_2 + \ldots + c'_1 z_k$, dann werden τ_3, $t_2\tau_3$, $t_3\tau_3$, ... alle Substitutionen sein, welche dies thun, und sie werden sämtlich von einander verschieden sein u. s. w. Man erhält also alle möglichen r Substitutionen, indem man N mit der Anzahl der Substitutionen 1, τ_2, τ_3, ... multipliziert.

Für die Wahl von $a_1, b_1, \ldots c_1$; $a'_1, b'_1, \ldots c'_1$; ... besteht die Beschränkung, dass die Zahlen eines Systems mit m keinen gemeinsamen Teiler haben dürfen. Es giebt demnach $[m, k]$ solcher Systeme und ebensoviele Substitutionen τ_1, τ_2, τ_3, ... Folglich wird

$$r = [m, k]\, N.$$

Die Substitutionen t haben die Form

$$| z_1, z_2, \ldots z_k \quad z_1, \; a_2 z_1 + b_1 z_2 + \ldots + c_2 z_k, \ldots a_k z_1 + b_k z_2 + \ldots + c_k z_k | \; (\mathrm{mod.}\, m).$$

Da $a_2, a_3, \ldots a_k$ gar nicht in den Wert der Determinante Δ dieser Substitution eingehen, so können sie ganz willkürlich, d. h. auf m^{k-1} Arten gewählt werden; die $b, \ldots c$ unterliegen der Bedingung, dass

$$\begin{vmatrix} b_2, \ldots c_2 \\ \cdot \quad \cdot \quad \cdot \\ b_k, \ldots c_k \end{vmatrix}$$

relativ prim zu m wird. Ist die Anzahl der hierbei möglichen Systeme r', so findet sich

$$r = [m, k]\, m^{k-1}.\, r'.$$

Nun hat aber r' dieselbe Bedeutung für eine Substitution von $(k-1)$ Indices (mod. m), wie sie r für k Indices besass. Folglich ist

$$r = [m, k]\, m^{k-1}\, [m, k-1]\, m^{k-2}.\, r'',$$

wo r'' dieselbe Bedeutung für $(k-2)$ Indices besitzt, und so erhält man schliesslich

$$r = [m, k]\, m^{k-1}.\, [m, k-1]\, m^{k-2}.\ \ldots\ [m, 2]\, m\, .\, r^{(k-1)}.$$

Es bezieht sich $r^{(k-1)}$ auf einen einzigen Index und ist also $= [m, 1]$. So wird

9) $$r = [m, k]\, m^{k-1}.\, [m, k-1]\, m^{k-2}.\ \ldots\ [m, 2]\, m\, .\, [m, 1].$$

§ 142. Das Symbol $[m, k]$ darzustellen, macht wenig Schwierigkeiten. Wir begnügen uns damit, den einfachen Fall zu behandeln, in welchem m eine Primzahl $= p$ wird, da dieser allein in der Folge zur Verwendung kommt. Dann wird offenbar

10) $$[p, \varrho] = p^{\varrho} - 1,$$

da nur die Kombination 0, 0, ... 0 aus den p^{ϱ} Kombinationen ausgeschlossen zu werden braucht. Mit Hilfe von 10) wird 9)

11) $$\begin{aligned} r &= (p^k - 1)\, p^{k-1}\, (p^{k-1} - 1)\, p^{k-2} \ldots (p^2 - 1)\, p\, .\, (p-1) \\ &= (p^k - 1)\, (p^k - p)\, (p^k - p^2) \ldots (p^k - p^{k-1}).* \end{aligned}$$

§ 143. Die Gesamtheit der geometrischen Substitutionen bildet eine Gruppe, deren Ordnung durch 9), respektive 11) angegeben wird. Diese soll die lineare Gruppe heissen. Soll der Grad derselben besonders hervorgehoben werden, dann sprechen wir von der linearen Gruppe des Grades m^k.

Man erkennt, dass die lineare Gruppe des Grades m^k nur solche Substitutionen enthält, welche das Element $x_{0,0,\ldots 0}$ ungeändert lassen. Denn

$$a_1 z_1 + b_1 z_2 + \ldots + c_1 z_k \equiv z_1, \quad a_2 z_1 + b_2 z_2 + \ldots + c_2 z_k \equiv z_2, \ \ldots \quad (\text{mod. } m.)$$

hat für jedes mögliche System $a_\lambda, b_\lambda, \ldots c_\lambda$ die Lösung

$$z_1 = 0, \quad z_2 = 0, \ \ldots\ z_k = 0 \quad (\text{mod. } m).$$

---

* Galois: Liouville Journal (1) XI, 1846, p. 410.

Wir werden bei der algebraischen Auflösung der Gleichungen des Genaueren mit dieser Gruppe zu thun haben.

Lehrsatz IV. Die Gruppe der geometrischen Substitutionen oder die lineare Gruppe des Grades m^k besitzt die in 9) angegebene Ordnung. Ihre Substitutionen lassen sämtlich das Element $x_{0,0,\ldots 0}$ ungeändert. Ihre Substitutionen sind mit der Gruppe der arithmetischen Substitutionen vertauschbar.

Zweiter Abschnitt.

Anwendung der Substitutionentheorie auf die algebraischen Gleichungen.

Neuntes Kapitel.

Die Gleichungen zweiten, dritten und vierten Grades. Gruppe einer Gleichung. Resolventen.

§ 144. Soll die Gleichung zweiten Grades

1) $$x^2 - c_1 x + c_2 = 0$$

mit Hilfe von Wurzelausziehungen aus bekannten Grössen gelöst werden, so kann man diese Aufgabe auch folgendermassen darstellen: „Bekannt sind die elementaren symmetrischen Funktionen c_1, c_2 der Wurzeln x_1, x_2 von 1); es soll aus ihnen die zweiwertige Funktion x_1 mittels Wurzelausziehungen erlangt werden.“* Nun ist uns bereits bekannt (erstes Kapitel § 17, S. 16), dass es eine zweiwertige Funktion giebt, deren Quadrat einwertig, nämlich die Diskriminante wird. In unserem Falle erhalten wir

$$\sqrt{\Delta} = (x_1 - x_2),$$
$$\Delta = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = c_1^2 - 4c_2,$$
$$x_1 - x_2 = \sqrt{c_1^2 - 4c_2}.$$

Da es nur eine einzige Gattung zweiwertiger Funktionen giebt, so kann durch die eine, soeben erlangte, jede andere zweiwertige Funktion rational dargestellt werden. Für die linearen zweiwertigen Funktionen ergiebt sich

---

* Vergl. C. G. J. Jacobi: Observatiunculae ad theoriam aequationum pertinentes. Crelle Journal 14 p. 340.

$$\alpha_1 x_1 + \alpha_2 x_2 = \frac{\alpha_1 + \alpha_2}{2}(x_1 + x_2) + \frac{\alpha_1 - \alpha_2}{2}(x_1 - x_2)$$

$$= \frac{\alpha_1 + \alpha_2}{2} c_1 + \frac{\alpha_1 - \alpha_2}{2} \sqrt{c_1^2 - 4c_2},$$

speziell für $\alpha_1 = 1,\ \alpha_2 = 0;\ \alpha_1 = 0,\ \alpha_2 = 1,$

$$x_1 = \frac{c_1}{2} + \tfrac{1}{2}\sqrt{c_1^2 - 4c_2}, \quad x_2 = \frac{c_1}{2} - \tfrac{1}{2}\sqrt{c_1^2 - 4c_2}.$$

§ 145. Bei der Gleichung dritten Grades

$$x^3 - c_1 x^2 + c_2 x - c_3 = 0$$

ist die Frage nach der Auflösung nicht die nach der dreiwertigen Funktion x_1, sondern die nach den drei dreiwertigen Funktionen x_1, x_2, x_3; es wird also durch die Lösung der Gleichung auch die $3!$-wertige Funktion

$$\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3$$

bekannt, und diese liefert dann natürlich auch umgekehrt x_1, x_2, x_3 einzeln. Es ist somit durch Wurzelausziehungen der Übergang von den einwertigen Funktionen c_1, c_2, c_3 zu einer sechswertigen Funktion von x_1, x_2, x_3 zu machen.

Zuerst liefert uns die Quadratwurzel aus der Diskriminante

$$\Delta = (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2 = -(4c_2^3 + 27c_3^2) + 18c_1c_2c_3 + c_1^2c_2^2 - 4c_1^3c_3$$

die zweiwertige Funktion

$$\pm (x_1 - x_2)(x_1 - x_3)(x_2 - x_3);$$

alle zweiwertigen Funktionen sind durch sie rational ausdrückbar. Die weitere Frage ist nun die, ob es eine mehrwertige Funktion von drei Elementen giebt, von der eine Potenz zweiwertig wird. Diese Frage ist im dritten Kapitel § 60 bereits erledigt. Die sechswertige Funktion

$$\varphi_1 = x_1 + \omega^2 x_2 + \omega x_3 \quad \left(\omega = \frac{-1 + \sqrt{-3}}{2}\right)$$

liefert, in die dritte Potenz erhoben,

$$\varphi_1^3 = \tfrac{1}{2}(-2c_1^3 + 9c_1c_2 - 27c_3 + 3\sqrt{-3\Delta})$$

$$= \tfrac{1}{2}(S_1 + 3\sqrt{-3\Delta}).$$

Ferner wird, wenn φ_2 durch Vorzeichenänderung der $\sqrt{-3}$ aus φ_1 entsteht,

$$\varphi_2^3 = (x_1 + \omega x_2 + \omega^2 x_3)^3 = \tfrac{1}{2}(S_1 - 3\sqrt{-3\Delta}).$$

Man erhält hierdurch die beiden Ausdrücke

$$x_1 + \omega^2 x_2 + \omega x_3 = \sqrt[3]{\tfrac{1}{2}(S_1 + 3\sqrt{-3\Delta})},$$

$$x_1 + \omega x_2 + \omega^2 x_3 = \sqrt[3]{\tfrac{1}{2}(S_1 - 3\sqrt{-3\Delta})}.$$

Kombiniert man mit diesen beiden in geeigneter Weise noch

$$x_1 + x_2 + x_3 = c_1,$$

und beachtet die Relation

$$1 + \omega + \omega^2 = 0,$$

so ergeben sich die Resultate

$$x_1 = \tfrac{1}{3}\left[c_1 + \sqrt[3]{\tfrac{1}{2}(S_1 + 3\sqrt{-3\Delta})} + \sqrt[3]{\tfrac{1}{2}(S_1 - 3\sqrt{-3\Delta})}\right],$$
$$x_2 = \tfrac{1}{3}\left[c_1 + \omega\sqrt[3]{\tfrac{1}{2}(S_1 + 3\sqrt{-3\Delta})} + \omega^2\sqrt[3]{\tfrac{1}{2}(S_1 - 3\sqrt{-3\Delta})}\right],$$
$$x_3 = \tfrac{1}{3}\left[c_1 + \omega^2\sqrt[3]{\tfrac{1}{2}(S_1 + 3\sqrt{-3\Delta})} + \omega\sqrt[3]{\tfrac{1}{2}(S_1 - 3\sqrt{-3\Delta})}\right].$$

Damit ist die Gleichung des dritten Grades gelöst.

§ 146. Bei der Gleichung vierten Grades

$$x^4 - c_1x^3 + c_2x^2 + c_3x + c_4 = 0$$

kennen wir gleichfalls wieder nur einwertige Funktionen c_1, c_2, c_3, c_4 und sollen die vier vierwertigen Funktionen x_1, x_2, x_3, x_4 und also auch die vierundzwanzigwertige Funktion

$$\alpha_1x_1 + \alpha_2x_2 + \alpha_3x_3 + \alpha_4x_4$$

durch successive Wurzelausziehungen berechnen.

Zuerst liefert die Quadratwurzel aus einer in den c_1, c_2, c_3, c_4 rationalen ganzen Funktion die zweiwertige Funktion $\sqrt{\Delta}$. Ferner haben wir in § 60 eine Funktion von sechs Werten

$$\varphi = (x_1x_2 + x_3x_4) + \omega(x_1x_3 + x_2x_4) + \omega^2(x_1x_4 + x_2x_3)$$

kennen gelernt, deren dritte Potenz zweiwertig wird und also zur Gattung von $\sqrt{\Delta}$ gehört. Sie kann daher aus einer zweiwertigen Funktion mit Hilfe einer Kubikwurzel berechnet werden. Mit ihr ist jede zu derselben Gattung gehörige Funktion bekannt. Die Gruppe von φ ist

$$G = [1, (x_1x_2)(x_3x_4), (x_1x_3)(x_2x_4), (x_1x_4)(x_2x_3)]; \quad \varrho = 6, \quad r = 4.$$

Zu derselben Gruppe gehört, und ist demnach durch φ rational ausdrückbar,

$$\psi^2 = (x_1x_2 - x_3x_4)^2(x_1x_3 + x_2x_4)^2,$$

während ψ, welches durch Quadratwurzelausziehung hieraus erlangt wird, zu

$$H = [1, (x_1x_2)(x_3x_4)]; \quad \varrho = 12, \quad r = 2$$

gehört. ψ kann demnach auch als bekannt gelten. Endlich werden

$$\chi^2 = [\alpha_1(x_1 - x_2) + \alpha_2(x_3 - x_4)]^2, \quad \omega = \beta_1(x_1 + x_2) + \beta_2(x_3 + x_4)$$

rational durch ψ ausdrückbar sein; χ wird nun eine vierundzwanzigwertige Funktion. Durch diese sind alle rationalen Funktionen der Wurzeln und speziell die Wurzeln selbst rational darstellbar. Man

kann diese erlangen, wenn man z. B. die vier Gleichungen, welche sich auf $\alpha_2 = +\alpha_1, -\alpha_1$; $\beta_2 = +\beta_1, -\beta_1$ beziehen, durch Addition und Subtraktion mit einander verbindet.

§ 147. Wollte man die Lösung der Gleichungen fünften Grades in ähnlicher Weise zu liefern unternehmen, so würde man nach unseren früheren Untersuchungen nicht über die Aufstellung zweiwertiger Funktionen hinauskommen. Denn wir sahen ja (§ 59), dass für mehr als vier von einander unabhängige Grössen $x_1, x_2, \ldots x_n$ keine mehrwertige Funktion besteht, von der eine Potenz zweiwertig würde. Bei diesem negativen Resultate bleibt es aber fraglich, ob nur ein Mangel der Methode die Auflösung der Gleichung verhindert, oder ob die Unmöglichkeit in der Natur der Sache begründet ist. Es wird sich zeigen, dass das letztere der Fall ist; wir werden nämlich die benutzte Methode später zu einer völlig naturgemässen durch den Beweis des Satzes erheben, dass jede bei der algebraischen Auflösung einer Gleichung auftretende irrationale Funktion der Koefficienten eine rationale Funktion der Wurzeln selbst ist; alle Schritte von der gegebenen einwertigen bis zu den gesuchten $n!$-wertigen Funktionen der Wurzeln können demnach durch die Theorie der ganzen rationalen Funktionen der Wurzeln verfolgt werden.

§ 148. Wir wollen uns zunächst noch mit der Präcisierung der Fragestellung bei der Auflösung von algebraischen Gleichungen beschäftigen.

Es sollen alle Wurzeln der Gleichung n^{ten} Grades

$$1) \qquad f(x) = 0$$

bestimmt werden. Ist eine derselben bekannt, so ist unsere Aufgabe nur zum Teil gelöst. Den noch übrigbleibenden Teil können wir mit Hilfe des bereits erledigten derart umformen, dass wir nicht mehr die übrigen $(n-1)$ Wurzeln der Gleichung 1) vom n^{ten} Grade, sondern wiederum alle Wurzeln einer Gleichung $(n-1)^{\text{ten}}$ Grades aufsuchen. Das Polynom $f(x)$ ist nämlich, wenn wir die bereits gefundene Wurzel mit x_1 bezeichnen, durch $x - x_1$ teilbar. Wir setzen

$$2) \qquad \frac{f(x)}{x - x_1} \equiv f_1(x) = x^{n-1} - \gamma_1 x^{n-2} + \gamma_2 x^{n-3} - \ldots + \gamma_{n-1} = 0.$$

Dann ist noch die Lösung von 2) zu bewerkstelligen. Kennt man eine Wurzel x_2 dieser neuen Gleichung, so lässt das noch übrigbleibende Problem in derselben Weise eine Umformung zu, indem wir zu der Gleichung

3) $$\frac{f_1(x)}{x-x_2} = f_2(x) = x^{n-2} - c_1 x^{n-3} + c_2 x^{n-4} - \ldots \pm c_{n-2} = 0$$

vom Grade $(n-2)$ übergehen. So kann man fortfahren, bis man zu einer Gleichung ersten Grades gelangt.

Man erkennt hierdurch, dass in der Aufgabe, eine Gleichung n^{ten} Grades zu lösen, eine Reihe von Problemen vereinigt liegt. Man kann diese einzelnen Aufgaben aber in eine einzige verwandeln, nämlich in die: eine einzige Wurzel einer gewissen Gleichung des Grades $n!$ zu finden.

Sind nämlich $x_1, x_2, \ldots x_n$, die von einander völlig unabhängigen Wurzeln der Gleichung 1), bekannt, so ist mit ihnen auch eine durch die willkürlichen Konstanten $\alpha_1, \alpha_2, \ldots \alpha_n$ bestimmte $n!$-wertige Funktion der Form

4) $$\xi = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$$

gegeben. Umgekehrt ist durch die Kenntnis von ξ eine jede Wurzel von 1) bekannt, da sich durch die $n!$-wertige Funktion ξ jede rationale Funktion von $x_1, x_2, \ldots x_n$ rational darstellen lässt.

Der Ausdruck von ξ genügt einer Gleichung

5) $$F(\xi) = \xi^{n!} + A_1 \xi^{n!-1} + \ldots = (\xi - \xi_1)(\xi - \xi_2) \ldots (\xi - \xi_{n!}) = 0$$

vom Grade $n!$, deren Koefficienten in denjenigen von 1) und in $\alpha_1, \alpha_2, \ldots \alpha_n$ ganz sind. Diese Gleichung ist im Gegensatze zu 1) eine sehr spezielle; denn ihre Wurzeln sind nicht mehr, wie dies bei 1) vorausgesetzt war, von einander unabhängig, sondern eine jede von ihnen kann durch jede andere rational dargestellt werden. Die vollständige Lösung von 5) und dann damit auch diejenige von 1) wird schon durch eine einzige Wurzel geliefert. Dies folgt daraus, dass, in Beziehung auf $x_1, x_2, \ldots x_n$, alle Werte $\xi_1, \xi_2, \ldots \xi_{n!}$ zu der Gruppe 1 gehören.

$F(\xi)$ heisst die Galois'sche Resolventengleichung von 1), ξ die Galois'sche Resolvente. Wir werden diese Benennung bald erweitern.

§ 149. Wir haben bisher lediglich von allgemeinen Gleichungen gesprochen, d. h. von solchen, deren Wurzeln $x_1, x_2, \ldots x_n$ von einander unabhängig sind. Die Betrachtung der Resolventengleichung $F(\xi) = 0$ führte uns bereits auf spezielle Gleichungen, d. h. auf solche, zwischen deren Wurzeln gewisse Beziehungen bestehen.

Wir wollen nachweisen, dass aus einer Beziehung, die zwischen den Wurzeln herrscht, eine solche zwischen den Koefficienten sich ergiebt.

Ist die zwischen $x_1, x_2, \ldots x_n$ bestehende Beziehung

6) $$\Phi_1(x_1, x_2, \ldots x_n) = 0,$$

so mögen die verschiedenen Ausdrücke, welche durch Anwendung der Substitutionen unter $x_1, x_2, \ldots x_n$ auf Φ_1 entstehen, $\Phi_1, \Phi_2, \ldots \Phi_\nu$ sein. Dann wird das Produkt

$$\prod_{\lambda=1}^{\nu} \Phi_\lambda(x_1, x_2, \ldots x_n)$$

wegen seines ersten Faktors verschwinden und wegen seiner symmetrischen Bildung in den Koefficienten $c_1, c_2, \ldots c_n$ von 1) rational sein. Wir setzen den Ausdruck gleich $\Psi(c_1 \ldots c_n)$ und erhalten

7) $$\Psi(c_1, c_2, \ldots c_n) = 0$$

aus 6). Sobald gezeigt ist, dass Ψ nicht identisch, d. h. für jede Wahl der c verschwindet, ist unser Satz als richtig erwiesen.

§ 150. Die höchste Potenz, in welcher irgend ein x in Φ_1 eingeht, sei die μ^{te}. Wir setzen:

S′$_m$) $\quad x_1 = a'_m,\ x_2 = b',\ x_3 = c', \ldots x_n = e' \quad (m = 1, 2, 3, \ldots \mu.n! + 1),$

wo die $a'_m, b', c', \ldots$ beliebige Grössen bedeuten. Berechnet man aus diesen $(\mu.n! + 1)$ Systemen die $c_1, c_2, \ldots c_n$, so wird bei identisch verschwindenden Ψ die Gleichung 7) gelten; also verschwindet jedesmal ein Faktor von $\prod_1^{\nu} \Phi_\lambda$ für jedes der $(\mu.n! + 1)$ Systeme S′$_m$). Da ν höchstens $= n!$ sein kann, so folgt, dass mindestens einer der Faktoren Φ_λ für $\mu + 1$ Systeme, die sich unter S′$_m$) befinden, gleich Null wird. Es sei dies Φ_α; wir ordnen diese Funktion nach Potenzen von x_1, $\Phi_\alpha = g_0^{(\alpha)}(x_2, \ldots x_n).x_1^{\mu} + g_1^{(\alpha)}(x_2, \ldots x_n).x_1^{\mu-1} + \ldots$

Die Systeme S′$_m$) lassen alle $g_0^{(\alpha)}, g_1^{(\alpha)}, \ldots$ ungeändert; $\mu + 1$ von ihnen liefern verschiedene x_1, durch welche $\Phi_\alpha = 0$ gemacht wird. Wir hätten daher eine Gleichung in x_1 mit $\mu + 1$ Wurzeln; d. h. die $g_0^{(\alpha)}, g_1^{(\alpha)}, \ldots$ werden für $x_2 = b', x_3 = c', \ldots$ verschwinden. Hätte man ein anderes System

S″$_m$) $\quad x_1 = a''_m,\ x_2 = b'',\ x_3 = c'', \ldots x_n = e'' \quad (m = 1, 2, \ldots n!\,\mu + 1)$

gewählt, so hätte man dieselben Schlüsse machen können, wäre dabei aber vielleicht auf eine andere Funktion Φ_β und die Koefficienten $g_0^{(\beta)}, g_1^{(\beta)}, \ldots$ gekommen. Nimmt man jedoch von solchen Systemen S′$_m$), S″$_m$), S‴$_m$) … mindestens $\mu.n! + 1$, so wird man auch mindestens $\mu + 1$ mal auf dasselbe Φ_γ und dieselben Koefficienten $g_0^{(\gamma)}$,

$g_1^{(\gamma)}, \ldots$ geführt werden. Wir können die Wahl der Systeme so treffen, dass alle $\mu . n! + 1$ in den Werten

$$8) \qquad x_3 = c', \quad x_4 = d', \ldots x_n = e'$$

übereinstimmen, während die Werte von x_2 sämtlich von einander verschieden sind. Ordnet man dann alle Funktionen $g_0^{(\gamma)}, g_1^{(\gamma)}, \ldots$ nach Potenzen von x_2, so werden die hierbei auftretenden Koefficienten, als Funktionen von $x_3, \ldots x_n$, ungeändert bleiben, während sämtliche $g_0^{(\gamma)}, g_1^{(\gamma)}, \ldots$ für mindestens $\mu + 1$ verschiedene Werte von x_2 verschwinden. Da x_2 nur in der μ^{ten} Potenz in die $g^{(\gamma)}$ eingehen kann, so sind die Koefficienten bereits durch 8) zu Null gemacht. Das heisst: Ordnet man alle Funktionen Φ nach Produkten $x_1^a x_2^b$, so verschwinden alle hierbei auftretenden Koefficienten einer der Funktionen Φ für ein beliebig gewähltes System 8). Nimmt man statt 8) ein anderes System, so kann die Funktion, deren Koefficienten verschwinden, eine andere werden; nimmt man dagegen wieder $\mu . n! + 1$ solcher Systeme, so tritt das Verschwinden mindestens bei einer Funktion für mindestens $\mu + 1$ System auf u. s. f.

So erkennt man, dass aus dem identischen Verschwinden von Ψ, das eines Φ also auch das von Φ_1 folgen würde. Dies verstösst jedoch gegen die Annahmen.

§ 151. Umgekehrt lässt sich jede Beziehung, die unter den Koefficienten $c_1, c_2, \ldots c_n$ von 1) besteht, in eine solche unter den $x_1, x_2, \ldots x_n$ umsetzen. Denn aus

$$\Phi(c_1, c_2, \ldots c_n) = 0$$

folgt

$$\Phi(x_1 + x_2 + \ldots + x_n,\ x_1 x_2 + x_1 x_3 + \ldots,\ \ldots) = \Psi(x_1, x_2, \ldots x_n) = 0.$$

Ψ ist nicht identisch Null. Denn da es symmetrisch ist, lässt es sich auf eine und auch nur auf eine Weise in eine Funktion von $c_1, c_2, \ldots c_n$ umwandeln, nämlich in $\Phi(c_1, c_2, \ldots c_n)$ (§ 9). Wäre $\Psi \equiv 0$, so wäre eine andere Umwandlung möglich, nämlich diejenige in den Ausdruck 0. Man hätte also auch Φ identisch gleich 0 zu setzen.

Es ist daher gleichgiltig, ob wir eine spezielle Gleichung als eine solche definieren, zwischen deren Wurzeln, oder als solche, zwischen deren Koefficienten eine Beziehung stattfindet. Denn eine jede der beiden Eigenschaften zieht die andere als Folge nach sich.

§ 152. Sind mehrere Beziehungen in Form von Gleichungen

$$\Phi_1(x_1, x_2, \ldots x_n) = 0, \quad \Phi_2(x_1, x_2, \ldots x_n) = 0, \ldots$$

unter den Wurzeln gegeben, so kann man diese mit Hilfe unbestimmter Koefficienten $\beta_1, \beta_2, \ldots$ in eine einzige verwandeln, nämlich in die Gleichung

$$\Phi = \Phi_1(x_1, x_2, \ldots x_n) \cdot \beta_1 + \Phi_2(x_1, x_2, \ldots x_n)\beta_2 + \ldots = 0.$$

Denn aus $\Phi = 0$ folgen jene einzelnen Gleichungen wieder, da jedes Φ_λ eine rationale Funktion von Φ ist (§ 99).

Dasselbe gilt, wenn mehrere Gleichungen zwischen den Koefficienten bestehen.

Wir können demgemäss sagen:

Jede spezielle Gleichung kann aus der allgemeinen durch Hinzunahme einer einzigen zwischen den Wurzeln $x_1, x_2, \ldots x_n$ bestehenden Beziehung

$$\Phi(x_1, \ldots x_n) = 0$$

abgeleitet werden.

Zu bemerken ist, dass Φ durch jede andere Funktion ersetzt werden kann, welche zur Gattung von Φ gehört. Denn zwischen beiden besteht gegenseitige rationale Ausdrückbarkeit. Ferner ist zu bemerken, dass es gleichgiltig ist, ob man Φ gleich Null setzt, oder ob man es als bekannt ansieht. Demgemäss ist es eine als bekannt angesehene Funktionengattung, welche den Spezialcharakter der Gleichung bestimmt. Man sagt, dass diese Gattung der Gleichung adjungiert sei. Endlich können wir auch diese Anschauung noch etwas ändern, indem wir statt der Funktionengattung die zugehörige Gruppe einführen. Zu jeder Gleichung gehört eine Gruppe derart, dass die zugehörige Funktionengattung als bekannt gilt. Eine allgemeine Gleichung ist folglich eine solche, deren Gruppe die symmetrische ist; denn lediglich die symmetrischen Funktionen der Wurzeln sind bei ihr bekannt.

§ 153. Wir wollen diese Festsetzungen und Anschauungen an einem Beispiele erläutern.

Es mögen alle Wurzeln einer irreduktiblen Gleichung $f(x) = 0$ rationale Funktionen einer einzigen unter ihnen sein:

$$x_2 = \varphi_2(x_1), \quad x_3 = \varphi_3(x_1), \ \ldots \ x_n = \varphi_n(x_1).$$

Dann erkennt man, dass die beiden Gleichungen

$$f(x) = 0 \quad \text{und} \quad f[\varphi_\lambda(x)] = 0$$

eine Wurzel gemeinsam haben, nämlich x_1; wegen der Irreduktibilität von $f(x)$ wird die zweite der beiden Gleichungen auch $x_2, \ldots x_n$, also die erste auch

$$\varphi_\lambda(x_2), \quad \varphi_\lambda(x_3), \ldots \varphi_\lambda(x_n),$$

d. h. allgemein jedes

$$\varphi_\alpha[\varphi_\beta(x_1)] \quad (\alpha, \beta = 2, 3, \ldots n)$$

zu Wurzeln haben. Wäre

$$\varphi_\alpha[\varphi_\gamma(x_1)] = \varphi_\beta[\varphi_\gamma(x_1)] \quad \alpha \neq \beta,$$

so hätten

$$f(x) = 0 \quad \text{und} \quad \varphi_\alpha(x) - \varphi_\beta(x) = 0$$

die Wurzel $\varphi_\gamma(x_1)$ also eine jede Wurzel der irreduktibeln Gleichung $f(x) = 0$ gemein. Dann wäre, was unmöglich ist, $\varphi_\alpha(x_1) = \varphi_\beta(x_1)$, d. h. es wären zwei Wurzeln von $f(x) = 0$ einander gleich. Es muss daher die Reihe

R_1) $\qquad x_\gamma, \quad \varphi_2(x_\gamma), \quad \varphi_3(x_\gamma), \ldots \varphi_n(x_\gamma)$

mit der Reihe

R_2) $\qquad x_1, \quad \varphi_2(x_1), \quad \varphi_3(x_1), \ldots \varphi_n(x_1)$

übereinstimmen, natürlich von der Aufeinanderfolge abgesehen.

Wenn man also eine Substitution auf die Reihe R_2) der Wurzeln von $f(x) = 0$ ausübt, welche x_1 in x_γ überführt, so geht dadurch jedes x_α in $\varphi_\alpha(x_\gamma)$ über; die Substitution ist daher durch die Angabe der einen Folge x_1, x_γ völlig bestimmt. Es giebt in unserem Falle demnach überhaupt nur n Substitutionen, deren Anwendung erlaubt ist; denn jede andere würde die über die Wurzeln gemachten Voraussetzungen zerstören. Diese Substitutionen bilden eine Gruppe Ω (§ 122): denn die Transitivität ist vorhanden, wie im folgenden Paragraphen gezeigt werden wird, und der Grad wie die Ordnung der Gruppe sind, wie eben bewiesen wurde, einander gleich und gleich n.

Diese Gruppe Ω ist die Gruppe unserer Gleichung.

Denn die Beziehungen, welche unsere Gleichung charakterisieren, gehen in

$$\Phi = \beta_2[x_2 - \varphi_2(x_1)] + \beta_3[x_3 - \varphi_3(x_1)] + \ldots + \beta_n[x_n - \varphi_n(x_1)] = 0$$

über. Wandelt man x_1 in x_γ um, so geht jedes x_α in $\varphi_\alpha(x_\gamma) = \varphi_\alpha[\varphi_\gamma(x_1)]$ über, genau wie bei der Anwendung der Gruppe Ω.

§ 154. Ohne fürs erste tiefer auf die Theorie der Gruppe einer Gleichung einzugehen, können wir doch zwei der wichtigsten Sätze bereits hier anführen.

Die Gruppe einer irreduktiblen Gleichung ist transitiv; ist die Gruppe einer Gleichung transitiv, so ist die Gleichung irreduktibel.

Ist die Gruppe G von

$$f(x) = (x - x_1)(x - x_2) \ldots (x - x_n) = 0$$

nicht transitiv, so mögen durch sie nur $x_1, x_2, \ldots x_\alpha$ mit einander verbunden sein; dann wird

$$\varphi(x) = (x - x_1)(x - x_2)\ldots(x - x_\alpha)$$

unter der Einwirkung von G ungeändert bleiben; φ gehört also zur Gattung der Gruppe G oder es steht unter ihr und ist jedenfalls bekannt; die Koefficienten von φ sind also durch bekannte Grössen darstellbar, und

$$\varphi(x) = 0$$

ist ein rationaler Teiler von $f(x) = 0$.

Ist umgekehrt $f(x)$ reduktibel, so wird ein $\varphi(x)$ der obigen Form rational bekannt sein; G enthält dann keine Substitution, welche x_1 in $x_{\alpha+1}$ umwandelt, da sonst eine bekannte Funktion $\varphi(x)$ nicht für alle Substitutionen von G ungeändert bleiben würde. Folglich ist G intransitiv.

Beide Sätze zusammengenommen geben das obige Theorem. —

Wir beweisen ferner: Die Ordnung der Gruppe einer irreduktiblen Gleichung vom Grade n, deren Wurzeln rationale Funktionen einer einzigen unter ihnen sind, ist gleich n; und umgekehrt: wenn die Gruppe einer Gleichung transitiv und ihre Ordnung ihrem Grade gleich ist, dann sind alle Wurzeln der Gleichung rationale Funktionen einer beliebigen unter ihnen.

Der erste Teil dieses Theorems ergiebt sich aus dem in § 153 behandelten Beispiele; den zweiten Teil weisen wir folgendermassen nach.

Aus der Transitivität der Gruppe folgt die Irreduktibilität der Gleichung.

Spezialisieren wir die vorgelegte Gleichung dadurch, dass wir ihr als neue Gattung diejenige adjungieren, welcher x_1 angehört, so reduziert sich die Gruppe. Sie enthält jetzt nur die Substitutionen, welche x_1 nicht ändern. Die Gruppe ist aber eine Gruppe Ω (§ 122); daher enthält sie nur eine Substitution, die Einheit, welche x_1 nicht ändert (§ 90). Bekannt sind also nach der Adjungierung von x_1 alle zur Gruppe 1 gehörigen oder unter ihr stehenden Funktionen. Speziell sind $x_2, x_3, \ldots x_n$ bekannt, d. h. rational durch x_1 darstellbar.

Hieraus folgt: Sind alle Wurzeln einer irreduktiblen Gleichung rationale Funktionen einer bestimmten Wurzel, so sind sie auch rationale Funktionen jeder beliebigen Wurzel.

§ 155. Im Falle einer allgemeinen Gleichung $f(x) = 0$ ist die zugehörige Galois'sche Resolventengleichung $F(\xi) = 0$ des Grades $n!$

irreduktibel. Es sind nämlich bei einer allgemeinen Gleichung nur die symmetrischen Funktionen der n Wurzeln $x_1, x_2, \ldots x_n$ bekannt; andererseits wird erst das Produkt der $n!$ Ausdrücke $(\xi - \xi_\lambda)$ symmetrisch.

Da jedes ξ_λ durch jedes andere rational ausdrückbar ist, so wird die Gruppe von $F(\xi) = 0$ Grad- und Ordnungszahl gleich haben, d. h. gleich $n!$ Um die Gruppe zu finden, schreiben wir alle Werte

$$\xi_1, \xi_2, \xi_3, \ldots \xi_{n!}$$

auf, wenden auf diese Reihe sämtliche Substitutionen von $x_1, x_2, \ldots x_n$ an und fassen die entstehenden Umsetzungen als Substitutionen unter den Elementen ξ auf. Da jede Substitution unter den x jeden Wert der $n!$-wertigen Funktion ξ umsetzt, so gehört die Gruppe der ξ zu den Gruppen Ω. Die Gruppe der x und die der ξ sind einander einstufig isomorph (§ 89). Als Beispiel wählen wir ein schon früher benutztes, welches durch die Gleichung dritten Grades geliefert wird; die Gruppen G und Γ von $f(x) = 0$ und $F(\xi) = 0$ sind

$$G = [1, (x_1 x_2), (x_1 x_3), (x_2 x_3), (x_1 x_2 x_3), (x_1 x_3 x_2)],$$
$$\Gamma = [1, (\xi_1 \xi_3)(\xi_2 \xi_4)(\xi_5 \xi_6), (\xi_1 \xi_6)(\xi_2 \xi_5)(\xi_3 \xi_4), (\xi_1 \xi_2)(\xi_3 \xi_5)(\xi_4 \xi_6),$$
$$(\xi_1 \xi_4 \xi_5)(\xi_2 \xi_3 \xi_6), (\xi_1 \xi_5 \xi_4)(\xi_2 \xi_6 \xi_3)].$$

Anders gestalten sich die Verhältnisse bei speziellen Gleichungen. Setzen wir wieder

$$4) \qquad \xi = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n,$$

so ist diese Funktion zwar nach wie vor $n!$-wertig; allein da nur die r Substitutionen der speziellen zur vorliegenden irreduktiblen Gleichung gehörigen Gruppe G in Anwendung gebracht werden dürfen, so besitzt für unsere Betrachtungen ξ auch nur r Werte. Sind diese

$$9) \qquad \xi_1, \xi_2, \ldots \xi_r,$$

so wird

$$10) \quad F_r(\xi) = (\xi - \xi_1)(\xi - \xi_2)\ldots(\xi - \xi_r) = \xi^r - B_1 \xi^{r-1} + \ldots = 0$$

die Galois'sche Resolvente der speziellen Gleichung. Ihre Gruppe Γ wird wie oben gefunden. Es ist eine Gruppe des Grades und der Ordnung r. Sie ist einstufig isomorph zu G.

Kennt man eine Wurzel ξ_1 von 10), so reduziert sich (vergl. § 154) die Gruppe Γ auf die identische Substitution 1. Dieser entspricht in der isomorphen Gruppe G dieselbe Substitution 1; alle Funktionen der speziellen Gleichung sind daher durch eine Wurzel $\xi_1 = \alpha_1 x_1 + \ldots + \alpha_n x_n$ rational ausdrückbar. Es spielt also ξ hier dieselbe Rolle, wie bei den allgemeinen Gleichungen.

Bezeichnen wir durch ξ'_1 einen der $n!$ Werte von ξ, welche in der Reihe 9) nicht vorkommen, so kann man mit demselben Rechte und aus denselben Gründen wie oben unter dem Einflusse der Gruppe G die r Werte

9') $\qquad \xi'_1, \xi'_2, \ldots \xi'_r$

entstehen lassen, und dann

10') $\qquad F'_r(\xi) \equiv (\xi - \xi'_1)(\xi - \xi'_2)\ldots(\xi - \xi'_r) = 0$

als Galois'sche Resolvente ansehen. $F_r(\xi)$ und $F'_r(\xi)$ gehören, als Funktionen von $x_1, x_2, \ldots x_n$ betrachtet, in der That zu derselben Gruppe, nämlich zu G. Die Gruppe Γ' von 10') ist eine Gruppe Ω; sie ist einstufig isomorph zu G, also auch zu Γ. Hieraus folgt nach dem Lehrsatze XXV) § 90, dass Γ und Γ' von gleichem Typus sind und sich nur durch die Bezeichnung von einander unterscheiden können.

Beide Funktionen $F_r(\xi)$ und $F'_r(\xi)$ sind Teiler der im allgemeinen Falle auftretenden Galois'schen Resolvente

5) $\qquad F(\xi) \equiv (\xi - \xi_1)(\xi - \xi_2)\ldots(\xi - \xi_{n!}).$

Wir erkennen daraus, dass bei allen speziellen Gleichungen die Funktion $F(\xi)$ reduktibel wird. Ist die spezielle Gleichung durch die Gattung der Gruppe G von der Ordnung r charakterisiert, so zerfällt 5) in $\varrho = \frac{n!}{r}$ Faktoren desselben Grades r. Dabei ist es gleichgiltig, welcher der Faktoren als Resolvente der besonderen Gleichung angesehen wird.

Man erkennt, dass der Übergang von $f(x) = 0$ zu $F_r(\xi) = 0$ identisch mit demjenigen von der Gruppe G zu der entsprechenden isomorphen Gruppe Γ ist, deren Grad- gleich ihrer Ordnungszahl wird.

§ 156. Den Ausdruck Resolvente können wir, allgemeiner als bisher, für eine jede mehrwertige Funktion verwenden, deren Elemente die Wurzeln der vorliegenden Gleichung $f(x) = 0$ sind. Eine ϱ-wertige Funktion $\varphi(x_1, x_2, \ldots x_n)$ ist insofern als eine Resolvente oder als eine resolvierende Funktion anzusehen, als durch die Auflösung einer Resolventengleichung des Grades ϱ das Problem der Lösung von $f(x) = 0$ vereinfacht wird. So hatten wir z. B. bei den Gleichungen vierten Grades folgendes System von Resolventen benutzt (§ 146):

1) die zweiwertige Funktion $\sqrt{\Delta} = (x_1 - x_2)(x_1 - x_3)\ldots(x_3 - x_4)$,
2) die sechswertige Funktion $\varphi = (x_1x_2 + x_3x_4) + \omega(x_1x_3 + x_2x_4) + \omega^2(x_1x_4 + x_2x_3)$,

3) die zwölfwertige Funktion $\psi = (x_1 x_2 - x_3 x_4)(x_1 x_3 + x_2 x_4)$,

4) die vierundzwanzigwertige Funktion $\chi = \alpha_1 (x_1 - x_2) + \alpha_2 (x_3 - x_4)$.

Anfänglich hatte die Gruppe der Gleichung die Ordnung 24; nach der Lösung der quadratischen Gleichung, deren Wurzel die zweiwertige Funktion $\sqrt{\Delta}$ war, reduzierte sich die allgemeine, symmetrische auf die alternierende Gruppe von der Ordnung 12. Eine Kubikwurzelausziehung führte uns auf die Gruppe G (§ 146) der Ordnung 4; eine Quadratwurzelausziehung auf die Gruppe H der Ordnung 2, und endlich kamen wir zur Gruppe 1 und damit zur definitiven Lösung der Gleichung, für welche die Benutzung von ω nicht nötig gewesen wäre.

Dass hierbei die Lösung einer Gleichung des Grades ϱ die Gruppe auf den ϱ^{ten} Teil der Substitutionen reduzierte, ist nicht auf beliebige Resolventen zu übertragen. Wir werden später sehen, dass dies bei den biquadratischen Gleichungen und der oben gewählten Resolventenfolge nur daher kam, weil die Gattung einer jeden vorhergehenden Resolvente eine ausgezeichnete Untergattung (§ 101) derjenigen der folgenden Resolvente war.

Ist eine ϱ-wertige Resolvente $\varphi(x_1, x_2, \ldots x_n)$ gegeben, so hängt dieselbe von einer Resolventengleichung ϱ^{ten} Grades

11) $$\varphi^\varrho - A_1 \varphi^{\varrho-1} + A_2 \varphi^{\varrho-2} - \ldots \pm A_\varrho = 0$$

ab. Um die zu dieser Gleichung gehörige Gruppe zu finden, schlagen wir dasselbe Verfahren ein, welches wir schon im vorigen Paragraphen benutzten.

Es mögen

$$\varphi_1, \varphi_2, \ldots \varphi_\varrho$$

die Werte sein, welche aus φ_1 entstehen, falls man auf diesen Wert alle Substitutionen der Gruppe G von $f(x) = 0$, anwendet. Jede Substitution von G wird die ϱ Werte φ unter einander vertauschen; dadurch erhält man verschiedene Komplexe, welche, als Substitutionen unter den φ aufgefasst, die zu 11) gehörige Gruppe konstituieren. Dieselbe ist isomorph zu G; sie ist ferner transitiv, da es in G Substitutionen geben wird, welche φ_1 in jedes andere φ_i umwandeln. Ist die Gruppe von φ_1 eine ausgezeichnete Untergruppe von G, so gehört sie auch zu $\varphi_2, \varphi_3, \ldots \varphi_\varrho$. Diese Werte sind somit durch φ_1 rational ausdrückbar. Also kommen wir nach § 154 auf eine Gruppe Ω.

§ 157. Man könnte versuchen, durch passend gewählte Resolventen die Reduktion und womöglich die Auflösung von 5) $F(\xi) = 0$ der Resolventengleichung des Grades $n!$ zu bewirken.* Trotzdem auf die-

* Dies versuchte Lagrange, Mem. d. Akad. d. W. zu Berlin; Band III.

sem Wege das gewünschte Ziel nicht zu erreichen ist, wie überhaupt auf keinem Wege, aus Gründen, die sich erst später entwickeln lassen, so sollen die betreffenden Untersuchungen doch in Kürze durchgeführt werden, weil sie für das bisher Besprochene passende Beispiele liefern.

Wir gehen wieder von der Gleichung

$$1) \qquad f(x) = 0$$

des Grades n aus. Es sei n eine zusammengesetzte Zahl, p einer ihrer Primzahlteiler und $n = m \cdot p$. Dann teilen wir die $n = m \cdot p$ Wurzeln in p Systeme von je m ganz nach Belieben gewählten Wurzeln, bilden die Summen der in jedem Systeme vorkommenden Wurzeln und benutzen diese zur Resolventenbildung:

$$\begin{aligned}
X_0 &= x_0 + x_p + x_{2p} + \ldots + x_{(m-1)p}, \\
X_1 &= x_1 + x_{p+1} + x_{2p+1} + \ldots + x_{(m-1)p+1}, \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
X_{p-1} &= x_{p-1} + x_{2p-1} + x_{3p-1} + \ldots + x_{mp-1}.
\end{aligned}$$

Dann bleibt die Gesamtheit der $X_0, X_1, \ldots X_{p-1}$ ungeändert, wenn wir nur solche Substitutionen ausführen, welche lediglich die in einem und demselben X_α vorkommenden x_λ unter sich vertauschen. Wir erhalten hierfür also eine intransitive Gruppe der Ordnung $(m!)^p$. Die symmetrischen Funktionen von $X_0, X_1, \ldots X_{p-1}$ bleiben ferner für die $p!$ unter den X_α möglichen Substitutionen ungeändert, infolgedessen auch für die entsprechende imprimitive, isomorphe Gruppe der x_λ von der Ordnung $p!\,(m!)^p$, bei welcher die x_λ jedes einzelnen Systems gleichzeitig ein System der Imprimitivität bilden. Diese symmetrischen Funktionen haben also $\varrho = \dfrac{n!}{p!\,(m!)^p}$ Werte, und sie gehören somit als Wurzeln einer Gleichung des Grades $\varrho = \dfrac{n!}{p!\,(m!)^p}$ an. Kennen wir eine Wurzel y_0 derselben, z. B. die, welche zu $X_0, X_1, \ldots X_{p-1}$ gehört, so kann man alle symmetrischen Funktionen dieser p Grössen rational darstellen; denn alle symmetrischen Funktionen von $X_0, X_1, \ldots X_{p-1}$ gehören zu derselben Gruppe. Wir sehen y_0 jetzt als bekannt an.

Als weitere Resolventen bilden wir unter Benutzung einer primitiven Wurzel ω der Gleichung $z^p - 1 = 0$ die cyklischen Funktionen

$$\begin{aligned}
\theta_1 &= (X_0 + \omega X_1 + \ldots + \omega^{p-1} X_{p-1})^p, \\
\theta_2 &= (X_0 + \omega^2 X_1 + \ldots + \omega^{2(p-1)} X_{p-1})^p, \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
\theta_{p-1} &= (X_0 + \omega^{p-1} X_1 + \ldots + \omega^{(p-1)^2} X_{p-1})^p.
\end{aligned}$$

Dann bleiben alle θ_α ungeändert für die n arithmetischen Substitutionen unter den X_α, welche jeden Index um dieselbe Zahl vermehren, und auch nur für diese Substitutionen (§ 137). Die symmetrischen Funktionen der θ bleiben ferner für diejenigen Substitutionen ungeändert, welche alle Indices mit einer und derselben Zahl multiplizieren (§ 126). Die Gruppe einer beliebigen symmetrischen Funktion von θ_1, θ_2, $\ldots \theta_{p-1}$ hat also die Ordnung $p(p-1)$; eine solche symmetrische Funktion der θ_α ist demnach aus den symmetrischen Funktionen der $X_0, X_1, \ldots X_{p-1}$, und folglich auch aus y_0 durch eine Gleichung des Grades $\frac{p!}{p.(p-1)} = (p-2)!$ ableitbar; auch von einer solchen Gleichung ist nur die Kenntnis einer einzigen Wurzel z_0 notwendig, um alle symmetrischen Funktionen der zugehörigen $p-1$ Grössen θ_α rational darstellen zu können.

Durch z_0 sind somit z. B. die elementaren symmetrischen Funktionen

$$\theta_1 + \theta_2 + \ldots + \theta_{p-1} = R_1(z_0),$$
$$\theta_1\theta_2 + \theta_1\theta_3 + \ldots + \theta_{p-2}\theta_{p-1} = R_2(z_0),$$
$$\ldots\ldots\ldots\ldots\ldots$$

ausdrückbar; durch Auflösung der Gleichung $(p-1)^{\text{ten}}$ Grades

$$\theta^{p-1} - R_1(z_0).\theta^{p-2} + R_2(z_0).\theta^{p-3} - \ldots = 0$$

kommt man auf die Werte θ_1, θ_2, $\ldots \theta_{p-1}$. Doch ist auch hier nur eine einzige Wurzel der Gleichung nötig, da alle Wurzeln zu derselben Gattung gehören und daher rational durch eine beliebige unter ihnen ausdrückbar sind.

Die Ausziehung der p^{ten} Wurzel aus θ_1 giebt

$$X_0 + \omega X_1 + \omega^2 X_2 + \ldots + \omega^{p-1} X_{p-1} = \sqrt[p]{\theta_1}.$$

Weil nun alle $\sqrt[p]{\theta_2}$, $\sqrt[p]{\theta_3}$, $\ldots$ zu derselben Gruppe der x_α von der Ordnung $(m!)^p$ gehören, wie $\sqrt[p]{\theta_1}$, so werden alle jene p^{ten} Wurzeln durch diese eine rational darstellbar sein. Man erhält demnach, wenn wir $\sqrt[p]{\theta_1} = u_0$ setzen und unter S_2, S_3, $\ldots$ gewisse rationale Funktionen verstehen, die Gleichungen:

$$X_0 + X_1 + X_2 + \ldots + X_{p-1} = S_1(y_0),$$
$$X_0 + \omega X_1 + \omega^2 X_2 + \ldots + \omega^{p-1} X_{p-1} = u_0,$$
$$X_0 + \omega^2 X_1 + \omega^4 X_2 + \ldots + \omega^{2p-1} X_{p-1} = S_2(u_0),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$X_0 + \omega^{p-1} X_1 + \omega^{2(p-1)} X_2 + \ldots + \omega^{(p-1)^2} X_{p-1} = S_{p-1}(u_0).$$

Durch einfache lineare Kombinationen ergeben sich

$$X_0 = \frac{1}{p}[S_1 + u_0 + S_2 + \ldots + S_{p-1}],$$

$$X_1 = \frac{1}{p}[S_1 + \omega^{-1}.u_0 + \omega^{-2}S_2 + \ldots + \omega^{-p+1}S_{p-1}],$$

. . . . . .

Um also bis zu den Resolventen X_0, X_1, ... X_{p-1} vorzudringen, braucht man nur zu kennen:

1) eine Wurzel y_0 einer Gleichung des Grades $\frac{n!}{p!(m!)^p}$;
2) eine Wurzel z_0 einer Gleichung des Grades $(p-2)!$, deren Koefficienten rational in y_0 darstellbar sind;
3) eine Wurzel θ_1 einer Gleichung des Grades $(p-1)$, deren Kofficienten rational in z_0 darstellbar sind;
4) eine p^{te} Wurzel u_0 aus der Grösse θ_1.

Das Produkt der Grade dieser Gleichungen

$$\frac{n!}{p!(m!)^p} \cdot (p-2)!(p-1).p = \frac{n!}{(m!)^p}$$

stimmt mit der Anzahl der Werte überein, welche eine lineare Kombination der X_0, X_1, ... bei Vertauschungen der x_i untereinander annehmen kann.

§ 158. Wäre $n = p$, so würde die erste der vier Gleichungen vom ersten Grade werden; sie fiele weg, und die X_α stimmten mit den Wurzeln x_α überein.

Unter diesen Umständen ist die Lösung der Gleichung identisch mit derjenigen von 2), 3), 4). Der Grad von 2), nämlich $(n-2)!$, übersteigt den Wert von n, sobald diese Zahl grösser wird als 4.

Wäre $n = p.m$, $(m > 1)$, so würden mit

$$X_0 = x_0 + x_p + x_{2p} + \ldots + x_{(m-1)p}$$

zugleich alle symmetrischen Funktionen der m Wurzeln

$$x_0,\ x_p,\ x_{2p},\ \ldots\ x_{(m-1)p}$$

bekannt sein, da sie sämtlich zur Gruppe von X_0 gehören.

Für $m = p_1 m_1$, wobei p_1 einen Primzahlteiler von m bedeutet, könnte man dieselbe Operation der Einteilung

$$Y_0 = x_0 + x_{p_1 p} + x_{2p_1 p} + \ldots$$
$$Y_1 = x_p + x_{(p_1+1)p} + x_{(2p_1+1)p} + \ldots$$
. . . . . .

wiederholen, und man käme durch ähnliche Gleichungen, wie die oben benutzten es waren, und durch deren Auflösung zu spezielleren Resolventen Y_0, Y_1, ... Wäre $m = p_1$, so hätte man durch diesen zwei-

ten Prozess p_1 Wurzeln der vorgelegten Gleichung erlangt. Ist $m_1 > 1$, so kann man in derselben Weise fortfahren.

§ 159. Durch dieses Verfahren von Lagrange ist zwar eine Vereinfachung in das Problem der Lösung der Resolventengleichung des Grades $n!$ gebracht, aber es ist weder ersichtlich, ob dasselbe die möglichste Reduktion des Problems giebt, noch inwieweit diese Methode bei den Gleichungen höherer Grade verwendbar ist.

Für die Gleichungen der ersten vier Grade führt sie direkt zur Lösung.

So bleiben bei den Gleichungen dritten Grades nur die Probleme 3) und 4) bestehen. Bei den Gleichungen vierten Grades liefert 1) den Grad $\frac{4!}{2!\,(2!)^2} = 3$; 2) den Grad 1; ebenso 3) den Grad 1; endlich 4) den Grad 2. Damit sind die Resolventen

$$X_0 = x_0 + x_2, \quad X_1 = x_1 + x_3$$

bekannt. Sind alle Wurzeln der Resolventengleichung dritten Grades bekannt, so sind auch

$$X'_0 = x_0 + x_1, \quad X'_1 = x_2 + x_3,$$
$$X''_0 = x_0 + x_3, \quad X''_1 = x_1 + x_2$$

gegeben. Für $n = 6$; $m = 3$, $p = 2$ hätte man den Grad $\frac{6!}{2!\,(3!)^2} = 10$ bei der Gleichung 1), für $n = 6$; $m = 2$, $p = 3$ den Grad $\frac{6!}{3!\,(2!)^3} = 15$. Hier, wie schon bei $n = 5$, kommt man zu Gleichungen von höherem als dem vorgelegten Grade.

Zehntes Kapitel.

Die Kreisteilungsgleichungen.

§ 160. Die Gleichung, welcher eine primitive p^{te} Einheitswurzel ω genügt (wo wie überall unter p eine Primzahl verstanden werden soll), führt den Namen „Kreisteilungsgleichung“; sie hat die Form

$$1) \qquad \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x^2 + x + 1 = 0.$$

Dann sind sämtliche Wurzeln von 1) die folgenden

$$2) \qquad \omega, \ \omega^2, \ \omega^3, \ \ldots \ \omega^{p-1}.$$

Wir beweisen, dass die linke Seite von 1) nicht als ein Produkt von zwei ganzen Funktionen $\varphi(x)$, $\psi(x)$ mit ganzzahligen Koefficienten dargestellt werden kann. Denn wäre dies der Fall, so ergäbe sich für $x = 1$

$$\varphi(1) . \psi(1) = p,$$

und einer der beiden ganzzahligen Faktoren z. B. $\varphi(1)$ müsste daher gleich ± 1 sein. Da ferner $\varphi(x) = 0$ mit 1) mindestens eine Wurzel gemeinsam hat, so wird

$$\varphi(\omega_1) . \varphi(\omega_1^2) . \varphi(\omega_1^3) \ldots \varphi(\omega_1^{p-1}) = 0$$

sein, wobei ω_1 eine beliebige der Wurzeln 2) bedeutet, und

$$\varphi(x) . \varphi(x^2) . \varphi(x^3) \ldots \varphi(x^{p-1}) = 0$$

hat also alle Grössen 2) zu Wurzeln; folglich ist die linke Seite dieser Gleichung durch die von 1) teilbar: es entsteht

3) $\varphi(x)\varphi(x^2) \ldots \varphi(x^{p-1}) = F(x) . (x^{p-1} + x^{p-2} + \ldots + x + 1)$,

wobei man unter $F(x)$ eine ganze Funktion mit ganzzahligen Koefficienten zu verstehen hat. Aus 3) wird für $x = 1$

$$\varphi(1)^{p-1} = p . F(1).$$

Es müsste also schliesslich $\varphi(1)^{p-1}$, welches den Wert Eins hat, durch p teilbar sein, was nicht möglich ist. Demnach ist 1) nicht reduktibel.

Lehrsatz I. Die Kreisteilungsgleichung für die Primzahl p

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

ist irreduktibel.

§ 161. Es sei nun g eine primitive Wurzel (mod. p), dann kann die Reihe 2) der Wurzeln der Kreisteilungsgleichung dargestellt werden als

4) $$\omega^g, \ \omega^{g^2}, \ \omega^{g^3}, \ \ldots \ \omega^{g^{p-1}}.$$

Da 1) irreduktibel ist, so ist die zugehörige Gruppe transitiv; es giebt also eine Substitution, welche ω^g in ω^{g^2} umwandelt. Dadurch geht

$$\omega^{g^\alpha} \quad \text{in} \quad (\omega^g)^{g^\alpha} = \omega^{g^{\alpha+1}}$$

über; die betreffende Substitution ist infolgedessen

$$s = (\omega^g \omega^{g^2} \omega^{g^3} \ldots \omega^{g^{p-1}}).$$

Die $p - 1$ Potenzen von s bilden die Gruppe von 1). Denn sie kommen in dieser Gruppe vor, und andrerseits hat diese nach § 154 nur $p - 1$ Substitutionen.

Wir stellen jetzt die cyklische Resolvente auf

$$(\omega + \alpha\omega^g + \alpha^2\omega^{g^2} + \ldots + \alpha^{p-2}\omega^{g^{p-2}})^{p-1},$$

in welcher α eine primitive Wurzel der Gleichung

$$z^{p-1} - 1 = 0$$

bedeuten soll. Nach unsern Auseinandersetzungen über cyklische Funktionen wird gemäss § 122 diese Resolvente für s und seine Potenzen, also für die Gruppe der Gleichung ungeändert bleiben. Es ist diese Resolvente demnach durch die Koefficienten von 1) und durch α rational darstellbar.

Wir bezeichnen ihren Wert durch T_1 und haben somit

$$5) \qquad \omega + \alpha\omega^g + \alpha^2\omega^{g^2} + \ldots + \alpha^{p-1}\omega^{g^{p-2}} = \sqrt[p-1]{T_1}.$$

Diese $(p-1)^{\text{te}}$ Wurzel aus T_1 ist eine möglichst vielwertige Funktion der Wurzeln 2); sie ist nämlich $(p-1)$-wertig, da sie für alle Substitutionen der Gruppe ihren Wert ändert. Ebensoviele Werte hat wegen der Vieldeutigkeit des Wurzelzeichens die rechte Seite.

Durch $\sqrt[p-1]{T_1}$ ist jede andere Funktion der Wurzeln rational darstellbar. Dies ergiebt sich aus der allgemeinen Theorie; wir wollen es aber hier in unserem besonderen Falle nochmals ableiten. Es bleibt für die Gruppe der Kreisteilungsgleichungen

$$6) \qquad (\omega + \alpha^\lambda\omega^g + \alpha^{2\lambda}\omega^{g^2} + \ldots)(\omega + \alpha\omega^g + \alpha^2\omega^{g^2} + \ldots)^{p-1-\lambda}$$

ungeändert, da der Einfluss von s diese Funktion in

$$\begin{aligned}
&(\omega^g + \alpha^\lambda\omega^{g^2} + \alpha^{2\lambda}\omega^{g^3} + \ldots)(\omega^g + \alpha\omega^{g^2} + \alpha^2\omega^{g^3} + \ldots)^{p-1-\lambda} \\
&\quad = \alpha^\lambda(\omega^g + \alpha^\lambda\omega^{g^2} + \alpha^{2\lambda}\omega^{g^3} + \ldots). \\
&\qquad \alpha^{p-1-\lambda}(\omega^g + \alpha\omega^{g^2} + \alpha^2\omega^{g^3} + \ldots)^{p-1-\lambda} \\
&\quad = (\omega + \alpha^\lambda\omega^g + \alpha^{2\lambda}\omega^{g^2} + \ldots)(\omega + \alpha\omega^g + \alpha^2\omega^{g^2} + \ldots)^{p-1-\lambda},
\end{aligned}$$

d. h. in sich selbst überführt. Dies thun dann auch die Potenzen von s; also gehört die Gruppe von 1) zu der aufgestellten Funktion 6). Bezeichnen wir daher diesen, durch α und die Koefficienten von 1) rational ausdrückbaren Wert 6) mit T_λ, dann erhält man für $\lambda = 1, 2, \ldots p-2$ die Reihe von Gleichungen

$$\begin{aligned}
&\omega + \alpha\omega^g + \alpha^2\omega^{g^2} + \ldots + \alpha^{p-2}\omega^{g^{p-2}} = \sqrt[p-1]{T_1}, \\
&\omega + \alpha^2\omega^g + \alpha^4\omega^{g^2} + \ldots + \alpha^{2(p-2)}\omega^{g^{p-2}} = \frac{T_2}{T_1}\sqrt[p-1]{T_1^2}, \\
&\qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&\omega + \alpha^{p-2}\omega^g + \alpha^{2(p-2)}\omega^{g^2} + \ldots + \alpha^{(p-2)^2}\omega^{g^{p-2}} = \frac{T_{p-2}}{T_1}\sqrt[p-1]{T_1^{p-2}}.
\end{aligned}$$

Verbindet man mit diesem Systeme die unmittelbar aus 1) folgende Beziehung

$$\omega + \omega^g + \omega^{g^2} + \ldots + \omega^{g^{p-2}} = -1,$$

so erhält man durch geeignete lineare Kombinationen

$$\omega = \frac{1}{p-1}\left[-1 + \sqrt[p-1]{T_1} + \frac{T_2}{T_1}\sqrt[p-1]{T_1^2} + \ldots + \frac{T_{p-2}}{T_1}\sqrt[p-1]{T_1^{p-2}}\right],$$

$$\omega^g = \frac{1}{p-1}\left[-1 + \alpha^{-1}\sqrt[p-1]{T_1} + \alpha^{-2}\frac{T_2}{T_1}\sqrt[p-1]{T_1^2} + \ldots + \alpha^{-p+2}\frac{T_{p-2}}{T_1}\sqrt[p-1]{T_1^{p-2}}\right],$$

$$\omega^{g^2} = \frac{1}{p-1}\left[-1 + \alpha^{-2}\sqrt[p-1]{T_1} + \alpha^{-4}\frac{T_2}{T_1}\sqrt[p-1]{T_1^2} + \ldots + \alpha^{-2p+4}\frac{T_{p-2}}{T_1}\sqrt[p-1]{T_1^{p-2}}\right],$$

. . . . . .

Es ist ersichtlich, wie eine Änderung der Wurzel α oder der Bedeutung von $\sqrt[p-1]{T_1}$ nur eine Vertauschung der Werte ω untereinander hervorruft.

Lehrsatz II. Um die Kreisteilungsgleichung für die Primzahl p aufzulösen, hat man eine primitive Wurzel der Gleichung $z^{p-1} - 1 = 0$ zu bestimmen, und aus einer hiernach rational darstellbaren Grösse die $(p-1)^{\text{te}}$ Wurzel zu ziehen. Die Kreisteilungsgleichung ist also auf zwei binomische Gleichungen des Grades $(p-1)$ reduzierbar.

§ 162. Die zweite der angegebenen Operationen kann man noch weiter vereinfachen. Es wird T_1 im allgemeinen complex und von der Form

$$T_1 = \varrho\,(\cos\vartheta + i\sin\vartheta)$$

sein. Führt man jetzt folgenden Ausdruck ein

$$\Theta_1 = (\omega^{-1} + \alpha^{-1}\omega^{-g} + \alpha^{-2}\omega^{-g^2} + \ldots)^{p-1},$$

so wird er, da ω und ω^{-1}, α und α^{-1} conjugierte Wurzeln sind, der conjugierte Ausdruck zu T_1 werden; man hat demnach

$$T_1 . \Theta_1 = \varrho\,(\cos\vartheta + i\sin\vartheta) . \varrho\,(\cos\vartheta - i\sin\vartheta)$$
$$= \varrho^2.$$

Ferner lässt sich, genau wie im vorigen Paragraphen, nachweisen, dass

$$\sqrt[p-1]{T_1\Theta_1} = (\omega + \alpha\omega^g + \alpha^2\omega^{g^2} + \ldots)\,(\omega^{-1} + \alpha^{-1}\omega^{-g} + \alpha^{-2}\omega^{-g^2} + \ldots)$$

zur Gruppe der Kreisteilungsgleichung gehört, und also rational durch α und die Koefficienten von 1) darstellbar ist. Es sei

$$\sqrt[p-1]{T_1\Theta_1} = U,$$

dann wird, falls man ϱ^2 für den Radikanden einsetzt:

$$\sqrt[p-1]{\varrho} = \sqrt[2]{U}.$$

Man erhält demnach für ein beliebiges ganzzahliges k

$$\sqrt[p-1]{T_1} = \sqrt[2]{U}\left(\cos\frac{\vartheta + 2k\pi}{p-1} + i\sin\frac{\vartheta + 2k\pi}{p-1}\right).$$

Da sowohl U wie ϑ bekannt sind, so hat man:

Lehrsatz III. Um die Kreisteilungsgleichung aufzulösen, hat man eine primitive Wurzel der Gleichung $z^{p-1} - 1 = 0$ zu bestimmen, einen Winkel, welcher dann konstruiert werden kann, in $(p-1)$ gleiche Teile zu teilen und aus einer bekannten Grösse die Quadratwurzel zu ziehen.

Diese bekannte Grösse, U nämlich, lässt sich leicht berechnen. Es ist

$$U = (\omega + \alpha\omega^g + \alpha^2\omega^{g^2} + \ldots + \alpha^{p-2}\omega^{g^{p-2}}).$$
$$(\omega^{-1} + \alpha^{-1}\omega^{-g} + \alpha^{-2}\omega^{-g^2} + \ldots + \alpha^{-p+2}\omega^{-g^{p-2}}).$$

Wir führen die Multiplikation derart durch, dass wir zuerst je zwei an entsprechenden Stellen der beiden Klammern befindliche Summanden mit einander multiplizieren. Das Resultat ist

$$1 + 1 + 1 + \ldots + 1 = p - 1.$$

Dann multiplizieren wir jedes Glied der ersten Klammer $\alpha^\lambda\omega^{g^\lambda}$ mit dem rechts benachbarten seines entsprechenden Gliedes in der zweiten Klammer, $\alpha^{-\lambda-1}\omega^{-g^{\lambda+1}}$; die Summe der Produkte ist

$$\alpha^{-1}(\omega^{-g+1} + \omega^{-g^2+g} + \omega^{-g^3+g^2} + \ldots).$$

Multiplizieren wir weiter jedes $\alpha^\lambda\omega^{g^\lambda}$ der ersten Klammer mit dem $\alpha^{-\lambda-2}\omega^{-g^{\lambda+2}}$ der zweiten Klammer und fahren nach derselben Methode fort, bis das Produkt U erlangt ist, so ergeben sich dabei die folgenden Unterprodukte, deren Summe zu bilden sein wird:

$$\alpha^{-1}(\omega^{-g+1} + \omega^{-g^2+g} + \omega^{-g^3+g^2} + \ldots),$$
$$\alpha^{-2}(\omega^{-g^2+1} + \omega^{-g^3+g} + \omega^{-g^4+g^2} + \ldots),$$
$$\alpha^{-3}(\omega^{-g^3+1} + \omega^{-g^4+g} + \omega^{-g^5+g^2} + \ldots),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

Nun ist $\omega^{-g^\delta+1}$ eine von 1 verschiedene p^{te} Einheitswurzel ω_1; denn es könnte nur dann

$$\omega^{-g^\delta+1} = 1$$

sein, wenn $-g^\delta + 1 = 0$, $g^\delta = 1 \pmod{p}$, also $\delta = 0$ oder gleich $p-1$ wäre. Wir können daher die Klammer der δ^{ten} Zeile durch

$$\omega_1 + \omega_1^g + \omega_1^{g^2} + \ldots + \omega_1^{g^{p-2}} = \frac{\omega_1^{g^{p-1}} - 1}{\omega_1 - 1} - 1 = -1$$

ersetzen und erhalten

$$U = (p-1) - (\alpha^{-1} + \alpha^{-2} + \ldots + \alpha^{-p+2}) = (p-1) - (-1)$$
$$= p.$$

Es folgt also:

Lehrsatz IV. Die Grösse, aus welcher nach der Vorschrift von Lehrsatz III) die Quadratwurzel zu ziehen ist, hat den Wert p.

§ 163. Durch das bisher besprochene Verfahren erhielt man, weil die Resolvente 5) $(p-1)$-wertig war, sofort die vollständige Lösung der Kreisteilungsgleichung. Mit Hilfe von minderwertigen Resolventen kann man die Lösung auf ihre einfachsten Bestandteile reduzieren.

Es sei p_1 ein Primzahlteiler von $p-1$, und $p_1 . q_1 = p-1$. Dann bilde man

$$(\omega + \alpha_1 \omega^g + \alpha_1^2 \omega^{g^2} + \ldots + \alpha_1^{p-2} \omega^{g^{p-2}})^{p_1},$$

worin α_1 eine primitive Wurzel der Gleichung

$$z^{p_1} - 1 = 0$$

bedeutet. Da $\alpha_1, \alpha_1^2, \ldots \alpha_1^{p_1}$ von einander verschieden sind, während die folgenden Potenzen von α_1 wieder dieselben Werte annehmen, so können die höheren Potenzen $\alpha_1^{p_1+1}, \ldots \alpha_1^{p-2}$ durch jene niederen ersetzt werden, und wenn man

$$\begin{aligned}
\varphi_0 &= \omega + \omega^{g^{p_1}} + \omega^{g^{2p_1}} + \ldots + \omega^{g^{(q_1-1)p_1}},\\
\varphi_1 &= \omega^g + \omega^{g^{p_1+1}} + \omega^{g^{2p_1+1}} + \ldots + \omega^{g^{(q_1-1)p_1+1}},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\varphi_{p_1-1} &= \omega^{g^{p_1-1}} + \omega^{g^{2p_1-1}} + \omega^{g^{3p_1-1}} + \ldots + \omega^{g^{p_1 q_1 - 1}}
\end{aligned}$$

setzt, so wird man die obige Resolvente schreiben können:

$$(\varphi_0 + \alpha_1 \varphi_1 + \alpha_1^2 \varphi_2 + \ldots + \alpha_1^{p_1-1} \varphi_{p_1-1})^{p_1}.$$

Es kann jetzt durch die früher benutzte Methode bewiesen werden, dass diese Resolvente sich beim Einsetzen von ω^g für ω nicht ändert, dass sie also zur Gruppe der Gleichung 1) gehört und demnach rational durch α_1 und die Koefficienten von 1) darstellbar ist. Wir bezeichnen ihren Wert mit $U_1^{(p_1)}$ und erhalten

$$\varphi_0 + \alpha_1 \varphi_1 + \alpha_1^2 \varphi_2 + \ldots + \alpha_1^{p_1-1} \varphi_{p_1-1} = \sqrt[p_1]{U_1^{(p_1)}}.$$

Setzt man dann, wieder genau wie oben,

$$\begin{aligned}
&(\varphi_0 + \alpha_1^{\lambda} \varphi_1 + \alpha_1^{2\lambda} \varphi_2 + \ldots + \alpha_1^{(p_1-1)\lambda} \varphi_{p_1-1}) .\\
&(\varphi_0 + \alpha_1 \varphi_1 + \alpha_1^2 \varphi_2 + \ldots + \alpha_1^{p_1-1} \varphi_{p_1-1})^{p_1-1-\lambda}\\
&\qquad = U_{\lambda}^{(p_1)},
\end{aligned}$$

so findet sich, dass $U_{\lambda}^{(p_1)}$ rational bekannt, und dass

$$\varphi_0 = \frac{1}{p_1}\left[-1 + \sqrt[p_1]{U_1^{(p_1)}} + \frac{U_2^{(p_1)}}{U_1^{(p_1)}}\sqrt[p_1]{U_1^{(p_1)^2}} + \ldots\right],$$

$$\varphi_1 = \frac{1}{p_1}\left[-1 + \alpha_1^{-1}\sqrt[p_1]{U_1^{(p_1)}} + \alpha_1^{-2}\frac{U_2^{(p_1)}}{U_1^{(p_1)}}\sqrt[p_1]{U_1^{(p_1)^2}} + \ldots\right],$$

. . . . . .

wird. Diese einzelnen Funktionen bleiben für die Einsetzung von $\omega^{g^{p_1}}$ statt ω also für die Potenzen

$$s^{p_1},\ s^{2p_1},\ s^{3p_1},\ \ldots\ s^{q_1 p_1}$$

ungeändert. Man erkennt:

Lehrsatz V. Die p_1-wertigen Resolventen $\varphi_0, \varphi_1, \ldots \varphi_{p_1-1}$ der Kreisteilungsgleichung gehören zu der aus den Potenzen von s^{p_1} gebildeten Gruppe. Man kann sie durch Aufsuchung einer primitiven Wurzel von $z^{p_1} - 1 = 0$ und Ausziehung einer p_1^{ten} Wurzel aus einer dann rational bekannten Grösse bestimmen.

Ist p_2 ein zweiter Primzahlteiler von $p-1$, und $p-1 = p_1 \cdot p_2 \cdot q_2$, so ist die Resolvente

$$(\omega + \alpha_2\omega^{g^{p_1}} + \alpha_2^{\,2}\omega^{g^{2p_1}} + \ldots + \alpha_2^{q_1-1}\omega^{g^{(q_1-1)p_1}})^{p_2},$$

in welcher α_2 eine primitive p_2^{te} Einheitswurzel bedeutet, auf die Form

$$(\chi_0 + \alpha_2\chi_1 + \alpha_2^{\,2}\chi_2 + \ldots + \alpha_2^{p_2-1}\chi_{p_2-1})^{p_2}$$

reduzierbar, wo unter

$$\chi_0 = \omega + \omega^{g^{p_1 p_2}} + \omega^{g^{2p_1 p_2}} + \ldots,$$

$$\chi_1 = \omega^{g^{p_1}} + \omega^{g^{p_1(p_2+1)}} + \omega^{g^{p_1(2p_2+1)}} + \ldots,$$

. . . . . .

verstanden werden muss. Man erkennt, dass diese Resolvente für den Übergang von ω zu $\omega^{g^{p_1}}$, also für die Substitutionen $s^{p_1}, s^{2p_1}, \ldots$ ungeändert bleibt und daher durch φ_0 rational darstellbar ist, wenn man α_2 als gegeben ansieht. Setzt man

$$(\chi_0 + \alpha_2^{\lambda}\chi_1 + \alpha_2^{\,2\lambda}\chi_2 + \ldots)\cdot(\chi_0 + \alpha_2\chi_1 + \alpha_2^{\,2}\chi_2 + \ldots)^{p_2-1-\lambda} = U_\lambda^{(p_2)},$$

so ist auch $U^{(p_2)}$ rational in φ_0, und es wird

$$\chi_0 = \frac{1}{p_2}\left[-\varphi_0 + \sqrt[p_2]{U_1^{(p_2)}} + \frac{U_2^{(p_2)}}{U_1^{(p_2)}}\sqrt[p_2]{U_1^{(p_1)^2}} + \ldots\right],$$

$$\chi_1 = \frac{1}{p_2}\left[-\varphi_0 + \alpha_2^{-1}\sqrt[p_2]{U_1^{(p_2)}} + \alpha_2^{-2}\frac{U_2^{(p_2)}}{U_1^{(p_2)}}\sqrt[p_2]{U_1^{(p_2)^2}} + \ldots\right],$$

. . . . . .

Lehrsatz VI. Die $p_1 \cdot p_2$-wertigen Resolventen $\chi_0, \chi_1, \ldots \chi_{p_1 p_2 - 1}$ der Kreisteilungsgleichung gehören der durch die Potenzen von $s^{p_1 p_2}$ bestimmten Gruppe an. Man kann sie durch

die Aufsuchung einer primitiven Wurzel von $z^{p_2}-1=0$ und die Ausziehung einer p_2^{ten} Wurzel aus einer durch φ_0 und diese primitive Wurzel rational bekannten Grösse bestimmen.

§ 164. Da dieses Verfahren sich fortsetzen lässt, so folgt:

Lehrsatz VII. Ist $p-1=p_1\cdot p_2\cdot p_3\ldots$, so braucht man, um die Kreisteilungsgleichung für die Primzahl p aufzulösen, nur je eine primitive Wurzel von

$$z^{p_1}-1=0,\quad z^{p_2}-1=0,\quad z^{p_3}-1=0,\ldots$$

zu kennen, und hat dann der Reihe nach eine p_1^{te}, p_2^{te}, p_3^{te}, ... Wurzel aus je einem Ausdrucke auszuziehen, welcher durch die vorhergehenden bekannten Grössen rational ausdrückbar ist.

Mit φ_0 sind gleichzeitig φ_1, φ_2, ... φ_{p_1-1} bekannt, da alle diese Funktionen zu derselben Gruppe gehören; ebenso kennt man die Koefficienten von

$$7)\quad \begin{cases} (x-\omega)(x-\omega^{g^{p_1}})(x-\omega^{g^{2p_1}})\ldots(x-\omega^{g^{(q_1-1)p_1}})=0, \\ (x-\omega^{g})(x-\omega^{g^{p_1}+1})(x-\omega^{g^{2p_1}+1})\ldots(x-\omega^{g^{(q_1-1)p_1}+1})=0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

Demgemäss zerfällt 1) nach der Durchführung des im Lehrsatz V) angegebenen Verfahrens in p_1 Faktoren 7). Da die zu einer jeden dieser neuen Gleichungen gehörige Gruppe in den betreffenden Wurzeln transitiv ist, so sind alle Faktoren 7) wiederum irreduktibel, so lange ausser den Koefficienten von 1) nur φ_0 als bekannt angesehen wird.

Nach der Durchführung des im Lehrsatze VI) angegebenen Verfahrens ist χ_0 bekannt. Da sämtliche Werte dieser Funktion zu einer und derselben Gruppe gehören, so sind sie auch sämtlich durch χ_0 darstellbar. Ebenso sind die Koefficienten von

$$8)\quad \begin{cases} (x-\omega)(x-\omega^{g^{p_1p_2}})(x-\omega^{g^{2p_1p_2}})\ldots(x-\omega^{g^{(q_2-1)p_1p_2}})=0, \\ (x-\omega^{g})(x-\omega^{g^{p_1p_2}+1})(x-\omega^{g^{2p_1p_2}+1})\ldots(x-\omega^{g^{(q_2-1)p_1p_2}+1})=0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

bekannt; jede der Gleichungen 7) wird also jetzt reduktibel und zerfällt in p_2 Faktoren 8), welche wiederum in dem durch χ_0 bestimmten Gebiete irreduktibel bleiben. In dieser Weise kann man fortfahren, bis man zu Gleichungen ersten Grades gelangt.

§ 165. Ein Spezialfall ist von besonderem Interesse; derjenige nämlich, für welchen alle Primfaktoren von $p-1$ gleich 2 sind.

Lehrsatz VIII. Ist 2^m+1 eine Primzahl p, so kann man die zu p gehörige Kreisteilungsgleichung mit Hilfe einer Reihe von m quadratischen Gleichungen auflösen. Das reguläre $p=2^m+1$ Eck ist in diesem Falle mit Hilfe von Zirkel und Lineal konstruierbar.

Es wird nämlich eine Wurzel der Kreisteilungsgleichung

$$\omega = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}, \quad \text{daher} \quad \omega^{-1} = \cos\frac{2\pi}{p} - i\sin\frac{2\pi}{p},$$

$$\omega + \omega^{-1} = 2\cos\frac{2\pi}{p};$$

demgemäss ist der Winkel $\frac{2\pi}{p}$ mit Zirkel und Lineal konstruierbar.

Damit 2^m+1 eine Primzahl sei, muss $m=2^\mu$ werden. Denn wäre $m=2^\mu.m_1$, wo m_1 eine ungerade Zahl ist, so würde

$$2^m+1=(2^{2^\mu})^{m_1}+1$$

durch $2^{2^\mu}+1$ teilbar sein, da für eine ungerade Zahl m_1

$$\frac{a^{m_1}+1}{a+1} = a^{m_1-1} - a^{m_1-2} + a^{m_1-3} - \ldots + 1$$

wird. Für

$$\mu = 0, 1, 2, 3, 4$$

findet man auch wirklich Primzahlen, nämlich

$$p = 3, 5, 17, 257, 65537;$$

für diese sind daher die entsprechenden p-Ecke konstruierbar. Für $\mu=5$ wird

$$2^{2^5}+1 = 4294967297 = 641 \cdot 6700417,$$

so dass es ungewiss bleibt, ob die Form 2^{2^μ} unendlich viele Primzahlen liefert.*

§ 166. Wir wollen für $p=5$ und $p=17$ die betreffenden Konstruktionen wirklich durchführen.

Für $p=5$ wählen wir die primitive Wurzel $g=2$ und erhalten

$$g^0 \equiv 1, \quad g^1 \equiv 2, \quad g^2 \equiv 4, \quad g^3 \equiv 3 \pmod 5.$$

* Vergl. Gauss: Disquisit. arithm. § 362. Die dort ausgesprochene Behauptung, Fermat habe gemeint, alle Zahlen $2^{2^\nu}+1$ seien Primzahlen, ist von Herrn R. Baltzer, Crelle's Journal 87, p. 172, berichtigt. – Bekannt sind als zerlegbar noch $2^{2^{12}}+1$ und $2^{2^{23}}+1$; ersteres ist durch 114689, letzteres durch 167772161 teilbar. Beide Resultate hat Herr J. Pervouchine, das zweite unabhängig von ihm auch Herr E. Lucas gefunden.

Demgemäss ist

$$\varphi_0 = \omega + \omega^4, \qquad \varphi_1 = \omega^2 + \omega^3,$$
$$\varphi_0 + \varphi_1 = -1, \quad \varphi_0 \varphi_1 = \varphi_0 + \varphi_1 = -1,$$
$$\varphi^2 + \varphi - 1 = 0,$$
$$\varphi_0 = \frac{-1+\sqrt{5}}{2}, \qquad \varphi_1 = \frac{-1-\sqrt{5}}{2}.$$

Da die Abänderung der Wurzel ω in ω^2 lediglich φ_0 und φ_1 mit einander vertauscht, so ist die Wahl des Vorzeichens bei φ_0 beliebig. Setzt man dagegen fest, dass

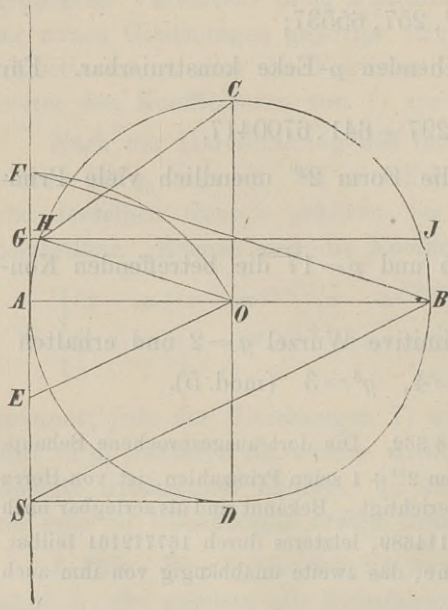
$$\omega = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$$

sein soll, so wird

$$\varphi_0 = \omega + \omega^4 = 2\cos\frac{2\pi}{5}, \qquad \varphi_1 = \omega^2 + \omega^3 = 2\cos\frac{4\pi}{5},$$

also $\varphi_0 > 0$, $\varphi_1 < 0$, und dann ergeben sich die Vorzeichen so, wie sie oben angenommen wurden. Weiter ist

$$\chi_0 = \omega, \quad \chi_1 = \omega^4; \quad \chi_2 = \omega^2, \quad \chi_3 = \omega^3;$$
$$\chi_0 + \chi_1 = \varphi_0, \quad \chi_0 \cdot \chi_1 = 1,$$
$$\chi^2 - \varphi_0 \chi + 1 = 0,$$
$$\chi_0 = \omega = \frac{-1+\sqrt{5}+i\sqrt{10+2\sqrt{5}}}{4}, \qquad \chi_1 = \omega^4 = \frac{-1+\sqrt{5}-i\sqrt{10+2\sqrt{5}}}{4}.$$



Die Wahl des Vorzeichens von i geschah so, dass der imaginäre Teil von ω positiv, der von ω^4 negativ wird.

Zur Konstruktion des regulären Fünfecks reicht die Kenntnis der Resolvente $\varphi_0 = 2\cos\frac{2\pi}{5}$ aus.

Es sei um O ein Kreis mit dem Radius 1 geschlagen; auf dem horizontalen Radius OA werde die Tangente errichtet und auf ihr $AE = \frac{1}{2}AO = \frac{1}{2}$ gemacht. Dann ist

$$OE = \sqrt{1+\tfrac{1}{4}} = \frac{\sqrt{5}}{2}.$$

Macht man dann $EF = EO$, so wird

$$AF = EO - EA = \frac{\sqrt{5}-1}{2} = \varphi_0,$$

$$AF = 2\cos\frac{2\pi}{5}.$$

Halbiert man endlich AF in G, zieht $GHJ \parallel OA$ und $OC \perp HJ$, dann wird $HOC = COJ = \frac{2\pi}{5}$ sein, weil $\cos HOC = AG = \cos\frac{2\pi}{5}$ ist. H, C, J sind daher drei aufeinander folgende Ecken eines regulären Fünfeckes.

§ 167. Für $p = 17$ ist $g = 6$ eine primitive Wurzel. Sie liefert:

$$g^0,\ g^1,\ g^2,\ g^3,\ g^4,\ g^5,\ g^6,\ g^7,\ g^8,\ g^9,\ g^{10},\ g^{11},\ g^{12},\ g^{13},\ g^{14},\ g^{15},\ g^{16};$$
$$1,\ 6,\ 2,\ 12,\ 4,\ 7,\ 8,\ 14,\ 16,\ 11,\ 15,\ 5,\ 13,\ 10,\ 9,\ 3,\ 1;$$
$$\varphi_0 = \omega + \omega^2 + \omega^4 + \omega^8 + \omega^{16} + \omega^{15} + \omega^{13} + \omega^9,$$
$$\varphi_1 = \omega^6 + \omega^{12} + \omega^7 + \omega^{14} + \omega^{11} + \omega^5 + \omega^{10} + \omega^3;$$
$$\varphi_0 + \varphi_1 = -1.$$

Um $\varphi_0 \cdot \varphi_1$ zu finden, multiplizieren wir in der Art, dass wir zuerst je zwei untereinander stehende Glieder multiplizieren; die Summe wird φ_1; dann multiplizieren wir jedes Glied von φ_0 mit demjenigen von φ_1, welches unter dem Nachbargliede zur Rechten steht; wir erhalten φ_0. Fahren wir in derselben Weise fort, so ergiebt sich

$$\varphi_0 \cdot \varphi_1 = \varphi_1 + \varphi_0 + \varphi_0 + \varphi_0 + \varphi_1 + \varphi_1 + \varphi_1 + \varphi_0 = 4(\varphi_0 + \varphi_1) = -4.$$

Es ist also

$$\varphi_0 + \varphi_1 = -1, \quad \varphi_0 \cdot \varphi_1 = -4,$$
$$\varphi^2 + \varphi - 4 = 0,$$
$$\varphi_0 = \frac{-1+\sqrt{17}}{2}, \quad \varphi_1 = \frac{-1-\sqrt{17}}{2},$$

wo das Vorzeichen beliebig ist, wenn die Wahl der Wurzel ω noch aussteht. Wenn jedoch

$$\omega = \cos\frac{2\pi}{17} + i\sin\frac{2\pi}{17}$$

angenommen wird, so ergiebt sich zur Bestimmung der Vorzeichens:

$$\varphi_1 = (\omega^3 + \omega^{14}) + (\omega^5 + \omega^{12}) + (\omega^6 + \omega^{11}) + (\omega^7 + \omega^{10})$$
$$= 2\left[\cos\frac{6\pi}{17} + \cos\frac{10\pi}{17} + \cos\frac{12\pi}{17} + \cos\frac{14\pi}{17}\right]$$
$$= 2\left[\cos\frac{6\pi}{17} - \cos\frac{7\pi}{17} - \cos\frac{5\pi}{17} - \cos\frac{3\pi}{17}\right] < 0$$

und dann sind die Zeichen so zu wählen, wie es oben geschehen ist. Ferner hat man

$$\chi_0 = \omega + \omega^4 + \omega^{16} + \omega^{13}, \qquad \chi_1 = \omega^2 + \omega^8 + \omega^{15} + \omega^9;$$
$$\chi_2 = \omega^6 + \omega^7 + \omega^{11} + \omega^{10}, \qquad \chi_3 = \omega^{12} + \omega^{14} + \omega^5 + \omega^3;$$
$$\chi_0 + \chi_1 = \varphi_0, \qquad \chi_2 + \chi_3 = \varphi_1;$$
$$\chi_0\chi_1 = \chi_3 + \chi_1 + \chi_0 + \chi_2 = -1, \qquad \chi_2\chi_3 = \chi_0 + \chi_3 + \chi_2 + \chi_1 = -1;$$
$$\chi^2 - \varphi_0\chi - 1 = 0, \qquad \chi^2 - \varphi_1\chi - 1 = 0;$$
$$\chi_0, \chi_1 = \frac{\varphi_0}{2} \pm \sqrt{\frac{\varphi_0^2+4}{4}}, \qquad \chi_2, \chi_3 = \frac{\varphi_1}{2} \pm \sqrt{\frac{\varphi_1^2+4}{4}}.$$

Die Verteilung der Vorzeichen ist auch hier leicht zu bestimmen. Man hat

$$\chi_0 = (\omega + \omega^{16}) + (\omega^4 + \omega^{13}) = 2\left(\cos\frac{2\pi}{17} + \cos\frac{8\pi}{17}\right) > 0,$$

$$\chi_2 = (\omega^6 + \omega^{11}) + (\omega^7 + \omega^{10}) = 2\left(\cos\frac{12\pi}{17} + \cos\frac{14\pi}{17}\right) < 0.$$

Danach wird

$$\chi_0 = \frac{\varphi_0}{2} + \sqrt{\frac{\varphi_0^2}{4}+1}, \quad \chi_1 = \frac{\varphi_0}{2} - \sqrt{\frac{\varphi_0^2}{4}+1};$$
$$\chi_2 = \frac{\varphi_1}{2} - \sqrt{\frac{\varphi_1^2}{4}+1}, \quad \chi_3 = \frac{\varphi_1}{2} + \sqrt{\frac{\varphi_1^2}{4}+1}.$$

Zerlegen wir weiter, indem wir uns auf χ_0 beschränken,

$$\psi_0 = \omega + \omega^{16}, \quad \psi_1 = \omega^4 + \omega^{13},$$
$$\psi_0 + \psi_1 = \chi_0, \quad \psi_0\psi_1 = \chi_3 = \frac{\varphi_1}{2} + \sqrt{\frac{\varphi_1^2}{4}+1},$$
$$\psi^2 - \chi_0\psi + \chi_3 = 0,$$
$$\psi_0, \psi_1 = \frac{\chi_0}{2} \pm \sqrt{\frac{\chi_0^2}{4} - \chi_3}.$$

Da nun $\psi_0 = 2\cos\frac{2\pi}{17}$, $\psi_1 = 2\cos\frac{8\pi}{17}$, also $\psi_0 > \psi_1$ ist, so erhält man

$$\psi_0 = \frac{\chi_0}{2} + \sqrt{\frac{\chi_0^2}{4} - \chi_3}, \quad \psi_1 = \frac{\chi_0}{2} - \sqrt{\frac{\chi_0^2}{4} - \chi_3}.$$

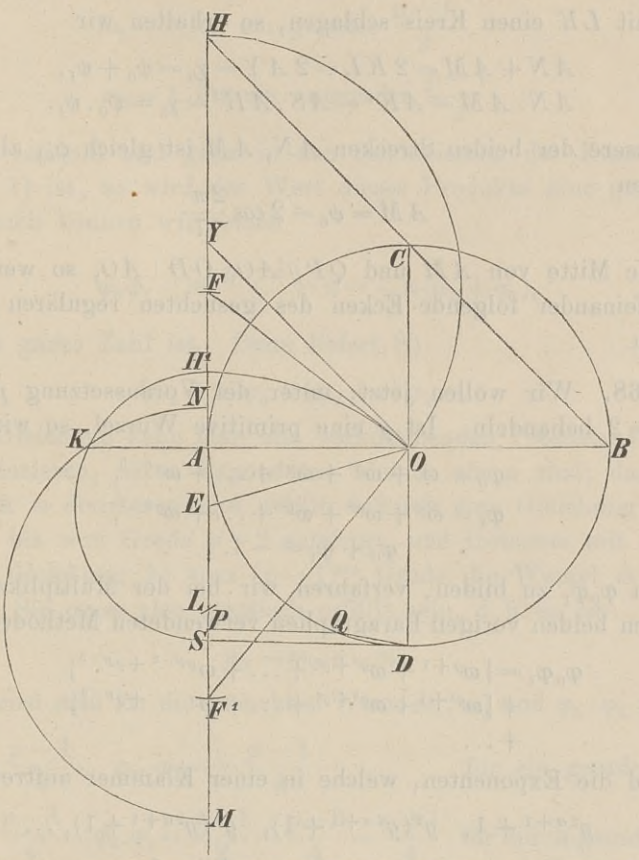
Diese Resultate reichen für die Konstruktion des regulären Siebzehnecks aus. Es sei um O mit dem Radius 1 ein Kreis geschlagen; auf dem horizontalen Radius OA werde eine Tangente errichtet und auf ihr $AE = \frac{1}{4}OA = \frac{1}{4}$ gemacht; dann ist:

$$OE = \sqrt{1 + \tfrac{1}{16}} = \frac{\sqrt{17}}{4}.$$

Ist ferner $EF = EF' = EO$, so wird

$$AF = \frac{\sqrt{17}-1}{4} = \frac{\varphi_0}{2}, \quad AF' = \frac{\sqrt{17}+1}{4} = -\frac{\varphi_1}{2};$$

$$OF = \sqrt{\frac{\varphi_0^2}{4}+1}, \qquad OF' = \sqrt{\frac{\varphi_1^2}{4}+1}.$$



Macht man

$$FH = FO,$$
$$F'H' = F'O,$$

so wird

$$AH = AF + FO = \frac{\varphi_0}{2} + \sqrt{\frac{\varphi_0^2}{4}+1} = \chi_0,$$

$$AH' = -AF' + F'O = \frac{\varphi_1}{2} + \sqrt{\frac{\varphi_1^2}{4}+1} = \chi_3.$$

AH halbieren wir in Y, so dass man erhält

$$AY = \tfrac{1}{2}\chi_0.$$

Jetzt machen wir $AS = 1$ und schlagen einen Halbkreis um $H'S$ als Durchmesser; dieser treffe die Verlängerung von OA in K; demnach folgt

$$AK^2 = AS.AH' = \chi_3.$$

Nehmen wir nun $LK = AY$ und dann $KL = LM = LN$, indem wir um L mit LK einen Kreis schlagen, so erhalten wir

$$AN + AM = 2KL = 2AY = \chi_0 = \psi_0 + \psi_1,$$
$$AN.AM = AK^2 = AS.AH' = \chi_3 = \psi_0 . \psi_1.$$

Die grössere der beiden Strecken AN, AM ist gleich ψ_0, also können wir setzen

$$AM = \psi_0 = 2\cos\frac{2\pi}{17}.$$

Ist P die Mitte von AM und $QP \parallel AO$, $OD \perp AO$, so werden Q, D zwei aufeinander folgende Ecken des gesuchten regulären Siebzehnecks sein.

§ 168. Wir wollen jetzt, unter der Voraussetzung $p > 2$, den Fall $p_1 = 2$ behandeln. Ist g eine primitive Wurzel, so wird

$$\varphi_0 = \omega + \omega^{g^2} + \omega^{g^4} + \ldots + \omega^{g^{p-3}},$$
$$\varphi_1 = \omega^g + \omega^{g^3} + \omega^{g^5} + \ldots + \omega^{g^{p-2}},$$
$$\varphi_0 + \varphi_1 = -1.$$

Um auch $\varphi_0\varphi_1$ zu bilden, verfahren wir bei der Multiplikation nach der in den beiden vorigen Paragraphen verwendeten Methode. Es wird

$$\varphi_0\varphi_1 = [\omega^{g+1} + \omega^{g^3+g^2} + \ldots + \omega^{g^{p-2}+g^{p-3}}]$$
$$+ [\omega^{g^3+1} + \omega^{g^5+g^2} + \ldots + \omega^{g \quad +g^{p-3}}]$$
$$+ \ldots$$

Hier sind die Exponenten, welche in einer Klammer auftreten,

$$g^{2\alpha+1}+1, \quad g^2(g^{2\alpha+1}+1), \quad g^4(g^{2\alpha+1}+1), \ldots$$

entweder sämtlich quadratische Reste, falls der erste es ist; oder sämtlich quadratische Nichtreste, falls der erste es ist; oder sämtlich gleich Null, falls der erste Null ist. Im ersten Falle ist der Wert der entsprechenden Klammer φ_0, im zweiten φ_1, im dritten $\frac{p-1}{2}$. Folglich wird

$$\text{S)} \quad \begin{cases} \varphi_0 . \varphi_1 = m_1 . \varphi_0 + m_2 . \varphi_1 + m_3 \dfrac{p-1}{2}, \\ m_1 + m_2 + m_3 = \dfrac{p-1}{2}, \end{cases}$$

wenn durch die Zahlen m_1, m_2, m_3 angegeben wird, wie oft die einzelnen Fälle eintreten.

Ist $g^{2\alpha+1}+1\equiv 0 \pmod{p}$, so wird $2(2\alpha+1)\equiv p-1$; es muss also $\frac{p-1}{2}$ eine ungerade Zahl sein; dann und nur dann kann der dritte Fall eintreten und zwar auch nur einmal, nämlich für $\alpha=\frac{p-3}{4}$. Daher ist

$$m_3=0 \text{ für ein gerades } \frac{p-1}{2},$$

$$m_3=1 \text{ für ein ungerades } \frac{p-1}{2}.$$

Da $\varphi_0.\varphi_1$ rational und ganz in den Koefficienten der Kreisteilungsgleichung 1) ist, so wird der Wert dieses Produkts eine ganze Zahl sein. Sonach können wir setzen

$$\varphi_0\varphi_1 - m_3\frac{p-1}{2} = n = -n(\varphi_0+\varphi_1),$$

wo n eine ganze Zahl ist. Dann liefert S)

$$(m_1+n)\varphi_0+(m_2+n)\varphi_1=0.$$

In dieser Gleichung kann man alle vorkommenden Potenzen von ω auf solche reduzieren, deren Exponenten kleiner als p sind; dann kann man durch ω dividieren und erhält dadurch eine Gleichung, welche höchstens bis zum Grade $p-2$ aufsteigt, und trotzdem mit der irreduktiblen Gleichung 1) vom $(p-1)^{\text{ten}}$ Grade die Wurzel ω gemeinsam hat. Sie muss also identisch erfüllt sein, d. h. es ist

$$m_1=m_2=-n.$$

Folglich wird man für die gesuchten Werte m_1, m_2 und $\varphi_0.\varphi_1$ erhalten:

$$m_1=m_2=\frac{p-1}{4},\quad \varphi_0.\varphi_1=-\frac{p-1}{4} \quad \text{für ein gerades } \frac{p-1}{2},$$

$$m_1=m_2=\frac{p-3}{4},\quad \varphi_0.\varphi_1=\frac{p-1}{2}-\frac{p-3}{4}=\frac{p+1}{4} \quad \text{für ein ungerades } \frac{p-1}{2},$$

$$\varphi_0\varphi_1=\frac{+1-(-1)^{\frac{p-1}{2}}p}{4},$$

$$(\varphi-\varphi_0)(\varphi-\varphi_1)=\varphi^2+\varphi+\frac{+1-(-1)^{\frac{p-1}{2}}p}{4},$$

$$\varphi_0=\frac{-1+\sqrt{(-1)^{\frac{p-1}{2}}p}}{2},\quad \varphi_1=\frac{-1-\sqrt{(-1)^{\frac{p-1}{2}}p}}{2},$$

wobei freilich über das der Quadratwurzel zu erteilende Vorzeichen nichts bekannt ist.

§ 169. Wir betrachten jetzt die beiden Gleichungen

$$z_0 \equiv (x-\omega)(x-\omega^{g^2})(x-\omega^{g^4})\ldots(x-\omega^{g^{p-3}}) = 0,$$
$$z_1 \equiv (x-\omega^{g})(x-\omega^{g^3})(x-\omega^{g^5})\ldots(x-\omega^{g^{p-2}}) = 0,$$

deren Koefficienten bei der Umwandlung von ω in ω^{g^2} ungeändert bleiben, weil dadurch die Wurzeln nicht geändert werden. Berechnet man somit irgend einen der Koefficienten, und erhält man bei der Ausführung der dazu nötigen Multiplikationen einen Summanden von der Form $m\omega^{\alpha}$, so muss derselbe Koefficient auch $m\omega^{\alpha g^2}$, $m\omega^{\alpha g^4}$, ... als Summanden enthalten, folglich $m\varphi_0$ oder $m\varphi_1$, jenachdem α ein quadratischer Rest oder Nichtrest mod. p ist. Demnach wird jeder Koefficient von der Form

$$m'\varphi_0 + m''\varphi_1 = \frac{a + b\sqrt{(-1)^{\frac{p-1}{2}}\cdot p}}{2}$$

werden und also wird durch Einführung dieser Ausdrücke als Koefficienten

$$z_0 = \frac{X + Y\sqrt{(-1)^{\frac{p-1}{2}}\cdot p}}{2},$$

wo unter X, Y ganze, ganzzahlige Funktionen von x verstanden sind. z_1 erhält man aus z_0 durch Umwandlung von ω in ω^{g}, oder von φ_0 in φ_1, also durch Änderung des Vorzeichens der Quadratwurzel; so entsteht der Ausdruck

$$z_1 = \frac{X - Y\sqrt{(-1)^{\frac{p-1}{2}}\cdot p}}{2}$$

und daraus

$$z_0 \cdot z_1 = \frac{x^p - 1}{x-1} = \frac{X^2 - (-1)^{\frac{p-1}{2}} p \cdot Y^2}{4},$$

und man hat das Resultat:

Lehrsatz IX. Es ist

$$4\left(\frac{x^p-1}{x-1}\right) = 4(x^{p-1} + x^{p-2} + \ldots + x + 1) = X^2 - (-1)^{\frac{p-1}{2}} p \cdot Y^2,$$

wo X und Y ganze, ganzzahlige Funktionen von x bedeuten.*

* Die reichhaltige zu diesem Kapitel gehörige Litteratur findet sich in: P. Bachmann, die Lehre von der Kreisteilung u. s. w., Leipzig, Teubner 1872. Wir sind der dort gewählten Darstellung in diesem Kapitel zum Teil gefolgt. Die beiden Figuren sind jenem Werke entnommen.

Elftes Kapitel.

Die Abel'schen Gleichungen.

§ 170. Die Kreisteilungsgleichung hat die Eigentümlichkeit, dass jede ihrer Wurzeln eine rationale Funktion jeder andern ist. Wir wenden uns jetzt zur Behandlung derjenigen irreduktiblen Gleichungen, bei denen eine Wurzel x'_1 eine rationale Funktion $\theta(x_1)$ einer anderen Wurzel x_1 der Gleichung ist. Es ist ersichtlich, dass diese Gleichungen die Kreisteilungsgleichungen als speziellen Fall umfassen.

Es sei

1) $$f(x) = 0$$

die gegebene irreduktible Gleichung; zwischen zweien ihrer Wurzeln x_1, x'_1 bestehe die Beziehung

2) $$x'_1 = \theta(x_1),$$

wo wir unter θ eine rationale Funktion verstehen. Dann ist

$$f(x_1) = 0, \quad f[\theta(x_1)] = 0,$$

so dass die irreduktible Gleichung 1) mit der Gleichung

3) $$f[\theta(x)] = 0$$

eine Wurzel gemeinsam hat. 3) wird daher für alle Wurzeln von 1) befriedigt werden; speziell wird $x'_1 = \theta(x_1)$ eine Wurzel von 3) sein. Aus

$$f\{\theta[\theta(x_1)]\} = 0$$

folgt dann weiter, dass $\theta[\theta(x_1)]$ eine Wurzel von 1) ist. Deshalb ist diese Grösse auch eine Wurzel von 3) und daher $\theta\{\theta[\theta(x_1)]\}$ eine solche von 1) u. s. w. Führen wir nun folgende Bezeichnungen ein:

$$\theta[\theta(x)] = \theta^2(x); \quad \theta[\theta^2(x)] = \theta^2[\theta(x)] = \theta^3(x), \ \ldots,$$

so erkennen wir, dass alle Glieder der unendlichen Reihe

$$x_1, \quad \theta(x_1), \quad \theta^2(x_1), \quad \theta^3(x_1), \ \ldots \ \theta^k(x_1), \ \ldots$$

Wurzeln der Gleichung 1) sind. Da diese aber nur eine endliche Anzahl von Wurzeln besitzt, so ergiebt sich durch eine vielfach benutzte Schlussweise, dass es in unserer Reihe eine Funktion $\theta^m(x_1)$ geben wird, welche dem Anfangswerte x_1 gleich ist, während alle ihr vorhergehenden Funktionen

$$x_1, \quad \theta(x_1), \quad \theta^2(x_1), \ \ldots \ \theta^{m-1}(x_1)$$

von einander verschieden sind. Diese ersten m Werte reproduzieren sich dann bei der Fortsetzung der Reihe, so dass z. B. nur die Glieder

$$x_1 = \theta^m(x_1) = \theta^{2m}(x_1) = \ldots$$

den Anfangswert annehmen, und dass für $k < m$ nur

$$\theta^k(x_1) = \theta^{m+k}(x_1) = \theta^{2m+k}(x_1) = \ldots$$

wird.

Giebt es ausserhalb des so erlangten Systems von m Wurzeln noch andere, welche der Gleichung 1) genügen, so sei x_2 eine solche. Auch diese befriedigt 3), also ist $\theta(x_2)$ eine Wurzel von 1) u. s. f. Wir finden daher hier eine Reihe von μ von einander verschiedenen Wurzeln

$$x_2,\ \theta(x_2),\ \theta^2(x_2),\ \ldots\ \theta^{\mu-1}(x_2).$$

Da die Gleichungen

4) $$\theta^m(y) - y = 0,\quad \theta^\mu(z) - z = 0$$

mit der irreduktiblen Gleichung 1) je eine Wurzel $y = x_1$, $z = x_2$ gemeinsam haben, so haben sie alle gemein mit ihr; die erste der Gleichungen 4) wird also durch x_2 befriedigt, die zweite durch x_1. Folglich ist m ein Vielfaches von μ und μ ein Vielfaches von m, d. h. es ist $m = \mu$.

Ferner sind alle Wurzeln der zweiten Reihe von denen der ersten Reihe verschieden. Denn aus der Annahme

$$\theta^b(x_2) = \theta^a(x_1) \quad (a,\ b < m)$$

würde durch Anwendung der Operation θ^{m-b} folgen

$$x_2 = \theta^m(x_2) = \theta^{m-b+a}(x_1),$$

d. h. es würde x_2 in der ersten Reihe vorkommen, was unseren Annahmen entgegen ist.

Sollte es ausser den $2m$ so erhaltenen Wurzeln noch eine andere x_3 geben, so wiederholen sich dieselben Schlussfolgerungen. Man erhält:

Lehrsatz I. Wenn eine Wurzel einer irreduktiblen Gleichung $f(x) = 0$ eine rationale Funktion einer anderen ist, so verteilen sich die Wurzeln in ν Reihen zu je m Wurzeln derart, dass die Tabelle

5)
$$\left|\begin{array}{l} x_1,\ \theta(x_1),\ \theta^2(x_1),\ \ldots\ \theta^{m-1}(x_1), \\ x_2,\ \theta(x_2),\ \theta^2(x_2),\ \ldots\ \theta^{m-1}(x_2), \\ \ldots\ldots\ldots\ldots\ldots \\ x_\nu,\ \theta(x_\nu),\ \theta^2(x_\nu),\ \ldots\ \theta^{m-1}(x_\nu) \end{array}\right.$$

entsteht. Hier ist für $\alpha = 1, 2, 3, \ldots \nu$

$$\theta^m(x_\alpha) = x_\alpha$$

und der Grad der Gleichung $f(x) = 0$ ist $m.\nu$.

Hiernach können wir die Gruppe der Gleichung 1) bestimmen. Über die Vertauschungen von $x_1, x_2, \ldots x_\nu$ unter einander ist durch die blosse Angabe, dass eine Wurzel eine rationale Funktion einer anderen sei, noch nichts vorgeschrieben. Es ist also jede Substitution unter $x_1, x_2, \ldots x_\nu$ erlaubt. Ersetzt man aber x_1 durch x_2, so geht die ganze erste Reihe von 5) in die zweite über u. s. f. Die Gruppe von 1) ist also imprimitiv. Sie hat ν Systeme der Imprimitivität zu je m Elementen. Die Vertauschungen der ν Systeme unter einander sind willkürlich. Setzt man dagegen für x_α ein $\theta^\lambda(x_\alpha)$, so geht $\theta^\varkappa(x)$ in $\theta^{\varkappa+\lambda}(x_\alpha)$ über. Innerhalb eines einzelnen Systems sind also nur m Substitutionen möglich. Die Ordnung der Gruppe von 1) ist also $r = \nu!\, m^\nu$.

Lehrsatz II. Die Gruppe der Gleichung 1) ist imprimitiv; sie enthält ν Systeme der Imprimitivität, die den einzelnen Zeilen von 5) entsprechen. Die Ordnung der Gruppe ist

$$r = \nu!\, m^\nu.$$

§ 171. Wir stellen jetzt folgende Resolventen auf:

$$\varphi_1 = x_1 + \theta(x_1) + \theta^2(x_1) + \ldots + \theta^{m-1}(x_1),$$
$$\varphi_2 = x_2 + \theta(x_2) + \theta^2(x_2) + \ldots + \theta^{m-1}(x_2),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\varphi_\nu = x_\nu + \theta(x_\nu) + \theta^2(x_\nu) + \ldots + \theta^{m-1}(x_\nu).$$

Wendet man auf φ_1 irgend eine derjenigen Substitutionen der Gruppe von 1) an, welche die Systeme der Imprimitivität ungeändert lässt, so bleibt auch φ_1 ungeändert; wendet man eine Substitution an, welche z. B. x_1 in $\theta^\lambda(x_\alpha)$ überführt, so geht zugleich damit

$$\theta(x_1) \text{ in } \theta^{\lambda+1}(x_\alpha), \quad \theta^2(x_1) \text{ in } \theta^{\lambda+2}(x_\alpha), \ldots$$

und demnach φ_1 in φ_α über. Es ist also φ_1 eine ν-wertige Funktion, und $\varphi_1, \varphi_2, \ldots \varphi_\nu$ sind ihre verschiedenen Werte. Die zu φ_1 gehörige Gruppe besteht aus den m^ν Substitutionen, welche die einzelnen Systeme nicht ändern, kombiniert mit denjenigen, welche die zu $\varphi_2, \varphi_3, \ldots \varphi_\nu$ gehörigen Systeme unter einander vertauschen; ihre Ordnung ist also $(\nu-1)!\, m^\nu$.

Jede symmetrische Funktion der φ ist in den Koefficienten von 1) rational darstellbar. Man hat also als bekannt anzusehen

$$S_1(\varphi_1) = \varphi_1 + \varphi_2 + \ldots + \varphi_\nu,$$
$$S_2(\varphi_1\varphi_2) = \varphi_1\varphi_2 + \varphi_1\varphi_3 + \ldots + \varphi_{\nu-1}\varphi_\nu,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

und somit sind die Koefficienten der Gleichung ν^{ten} Grades

6) $$\varphi^\nu - S_1 . \varphi^{\nu-1} + S_2 . \varphi^{\nu-2} - \ldots \pm S_\nu = 0,$$

von welcher $\varphi_1, \varphi_2, \ldots \varphi_\nu$ abhängen, bekannt. Ohne weitere spezialisierende Voraussetzungen über $x_1, x_2, \ldots x_\nu$ lässt sich von dieser Gleichung nichts Besonderes aussagen. Wir sehen:

Lehrsatz III. Die Resolvente

$$\varphi_1 = x_1 + \theta(x_1) + \theta^2(x_1) + \ldots + \theta^{m-1}(x_1)$$

hängt von einer Gleichung ν^{ten} Grades ab, deren Koefficienten rational durch diejenigen der Gleichung $f(x) = 0$ ausdrückbar sind.

§ 172. Nehmen wir an, auf irgend eine Weise wäre φ_1 uns bekannt geworden, dann kann die Rechnung genau nach der im vorigen Kapitel verwendeten Methode weiter geführt werden. Wir bilden, wie dort, eine cyklische Funktion

$$T_1 = [x_1 + \omega\theta(x_1) + \omega^2\theta^2(x_1) + \ldots + \omega^{m-1}\theta^{m-1}(x_1)]^m,$$

wobei ω eine primitive Wurzel der binomischen Gleichung

$$z^m - 1 = 0$$

sein soll. Ersetzt man in T_1 die Wurzel x_1 durch $\theta(x_1)$, so geht T_1 in

$$[\theta(x_1) + \omega\theta^2(x_1) + \ldots + \omega^{m-2}\theta^{m-1}(x_1) + \omega^{m-1}.x_1]^m$$
$$= \omega^m [\theta(x_1) + \omega\theta^2(x_1) + \ldots + \omega^{m-2}\theta^{m-1}(x_1) + \omega^{m-1}x_1]^m = T_1$$

über. T_1 bleibt also für alle Substitutionen ungeändert, die φ_1 nicht ändern, und daher hat man T_1 als rationale Funktion von φ_1 anzusehen.

Wir betrachten ferner den Ausdruck

$$(x_1 + \omega^\lambda\theta(x_1) + \omega^{2\lambda}\theta^2(x_1) + \ldots) . (x_1 + \omega\theta(x_1) + \omega^2\theta^2(x_1) + \ldots)^{m-\lambda};$$

dann weist sich auch dieser als zur Gruppe von φ_1 gehörig und demnach als durch φ_1 rational ausdrückbar aus. Wir setzen ihn gleich T_λ und finden

$$x_1 + \theta(x_1) + \theta^2(x_1) + \ldots + \theta^{m-1}(x_1) = \varphi_1,$$
$$x_1 + \omega\theta(x_1) + \omega^2\theta^2(x_1) + \ldots + \omega^{m-1}\theta^{m-1}(x_1) = \sqrt[m]{T_1},$$
$$x_1 + \omega^2\theta(x_1) + \omega^4\theta^2(x_1) + \ldots + \omega^{2m-2}\theta^{m-1}(x_1) = \frac{T_2}{T_1}\sqrt[m]{T_1^2},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Lineare Kombinationen dieser Gleichungen geben die Wurzelwerte

$$x_1 = \frac{1}{m}\left[\varphi_1 + \sqrt[m]{T_1} + \frac{T_2}{T_1}\sqrt[m]{T_1^2} + \ldots + \frac{T_{m-1}}{T_1}\sqrt[m]{T_1^{m-1}}\right],$$
$$\theta(x_1) = \frac{1}{m}\left[\varphi_1 + \omega\sqrt[m]{T_1} + \omega^2\frac{T_2}{T_1}\sqrt[m]{T_1^2} + \ldots + \omega^{m-1}\frac{T_{m-1}}{T_1}\sqrt[m]{T_1^{m-1}}\right],$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Lehrsatz IV. Sind

$$x_1,\ \theta(x_1),\ \theta^2(x_1),\ \ldots\ \theta^{m-1}(x_1)$$

die m Wurzeln einer Gleichung m^{ten} Grades, wobei $\theta(x)$ eine rationale Funktion bedeutet, für welche $\theta^m(x_1) = x_1$ ist, so kann man diese Gleichung auflösen, indem man eine primitive Wurzel von $z^m - 1 = 0$ bestimmt, und aus einer bekannten Grösse die m^{te} Wurzel zieht.

Lehrsatz V. Sind zwei Wurzeln einer irreduktiblen Gleichung eines Primzahlgrades so mit einander verbunden, dass die eine von ihnen als rationale Funktion der anderen darstellbar ist, so kann die Gleichung algebraisch gelöst werden.

Denn man hat $m.v = p$ und $m > 1$; folglich ist $m = p$ und $v = 1$.

Falls alle in $f(x)$ und in $\theta(x)$ vorkommenden Grössen reell sind, kann man hier weitere Reduktionen eintreten lassen, welche sich auf die Ausziehung der m^{ten} Wurzel beziehen. Man kann

$$T_1 = (x_1 + \omega\theta(x_1) + \omega^2\theta^2(x_1) + \ldots)^m = \varrho\,(\cos\vartheta + i\sin\vartheta)$$

durch die Koefficienten von f, θ, φ_1 und durch ω darstellen. Das Auftreten von $i = \sqrt{-1}$ kann unter unseren Voraussetzungen nur von ω herrühren, so dass

$$T_{m-1} = (x_1 + \omega^{-1}\theta(x_1) + \omega^{-2}\theta^2(x_1) + \ldots)^m = \varrho\,(\cos\vartheta - i\sin\vartheta)$$

und das Produkt der beiden conjugierten Grössen

$$T_1 . T_{m-1} = \varrho^2$$

wird. Andrerseits ist die m^{te} Wurzel aus diesem Produkte

$$\sqrt[m]{T_1 . T_{m-1}} = (x_1 + \omega\theta(x_1) + \omega^2\theta^2(x_1) + \ldots)(x_1 + \omega^{-1}\theta(x_1) + \omega^{-2}\theta^2(x_1) + \ldots)$$

für die Substitution von $\theta(x_1)$ statt x_1 unveränderlich und also durch bekannte Grössen rational darstellbar; es sei der Wert dieser m^{ten} Wurzel gleich U. Dann wird

$$\sqrt[m]{\varrho} = \sqrt[2]{U}$$

und

$$\sqrt[m]{T_1} = \sqrt[2]{U}\left(\cos\frac{\vartheta + 2k\pi}{m} + i\sin\frac{\vartheta + 2k\pi}{m}\right).$$

Lehrsatz VI. Die zweite der im Lehrsatz IV) angegebenen Operationen kann, falls alle in $f(x)$ und $\theta(x)$ vorkommenden Grössen reell sind, durch die Ausziehung einer Quadratwurzel aus einer bekannten Grösse und durch die Teilung eines bekannten Winkels in m gleiche Teile ersetzt werden.

§ 173. Ist die im Lehrsatze IV) angegebene Zahl m eine zusammengesetzte Zahl, so kann man speziellere Resolventen zur Lösung verwenden. Ist $m = m_1 . m'_1$, wo m_1 ein beliebiger Teiler von m sein mag, so setzen wir

$$\psi_1 = x_1 + \theta^{m_1}(x_1) + \theta^{2m_1}(x_1) + \ldots + \theta^{(m'_1-1)m_1}(x_1),$$
$$\psi_2 = \theta(x_1) + \theta^{m_1+1}(x_1) + \theta^{2m_1+1}(x_1) + \ldots + \theta^{(m'_1-1)m_1+1}(x_1),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\psi_{m_1} = \theta^{m_1-1}(x_1) + \theta^{2m_1-1}(x_1) + \theta^{3m_1-1}(x_1) + \ldots + \theta^{m'_1 m_1-1}(x_1),$$

und betrachten die Resolvente

$$[x_1 + \alpha_1\theta(x_1) + \alpha_1{}^2\theta^2(x_1) + \ldots + \alpha_1{}^{n-1}\theta^{n-1}(x_1)]^{m_1},$$

in welcher α_1 eine primitive $m_1{}^{\text{te}}$ Einheitswurzel bedeutet. Diese Resolvente ist gleich

$$(\psi_1 + \alpha_1\psi_2 + \alpha_1{}^2\psi_3 + \ldots + \alpha_1{}^{m_1-1}\psi_{m_1})^{m_1};$$

sie bleibt bei der Einsetzung von $\theta(x_1)$ statt x_1, durch welche die $\psi_1, \psi_2, \ldots \psi_{m_1}$ cyklisch verschoben werden, ungeändert und ist also durch α_1 und bekannte Grössen rational darstellbar; wir setzen diesen Ausdruck gleich $U_1^{(m_1)}$ und erhalten

$$\psi_1 + \alpha_1\psi_2 + \alpha_1{}^2\psi_3 + \ldots + \alpha_1{}^{m_1-1}\psi_{m_1} = \sqrt[m_1]{U_1^{(m_1)}}.$$

Nimmt man dann, wieder genau wie oben,

$$(\psi_1 + \alpha_1{}^\lambda\psi_2 + \alpha_1{}^{2\lambda}\psi_3 + \ldots + \alpha_1{}^{(m_1-1)\lambda}\psi_{m_1})(\psi_1 + \alpha_1\psi_2 + \alpha_1{}^2\psi_3 + \ldots)^{m_1-1-\lambda} = U_\lambda^{(m_1)},$$

so findet sich, dass $U_\lambda^{(m_1)}$ rational bekannt, und dass

$$\psi_1 = \frac{1}{m_1}\left[\varphi_1 + \sqrt[m_1]{U_1^{(m_1)}} + \frac{U_2^{(m_1)}}{U_1^{(m_1)}}\sqrt[m_1]{U_1^{(m_1)2}} + \ldots\right],$$
$$\psi_2 = \frac{1}{m_1}\left[\varphi_1 + \alpha_1{}^{-1}\sqrt[m_1]{U_1^{(m_1)}} + \alpha_1{}^{-2}\frac{U_2^{(m_2)}}{U_1^{(m_1)}}\sqrt[m_1]{U_1^{(m_1)2}} + \ldots\right],$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

wird.

Lehrsatz VII. Die m_1-wertige Resolvente ψ_1 kann erlangt werden, indem man eine primitive Wurzel von $z^{m_1} - 1 = 0$ aufsucht und aus einer bekannten Grösse die $m_1{}^{\text{te}}$ Wurzel zieht.

Da dieses Verfahren sich fortsetzen lässt, so folgt:

Lehrsatz VIII. Sind, unter θ eine rationale Funktion verstanden,

$$x_1,\ \theta(x_1),\ \theta^2(x_1),\ \ldots\ \theta^{m_1-1}(x_1) \quad [\theta^{m_1}(x_1) = x_1]$$

die Wurzeln einer Gleichung $m_1{}^{\text{ten}}$ Grades, so braucht man, wenn $m = m_1 . m_2 . m_3 \ldots$ ist, zur Auflösung dieser Gleichung nur je eine primitive Wurzel von

$$z^{m_1}-1=0,\quad z^{m_2}-1=0,\quad z^{m_3}-1=0,\ \ldots$$

zu kennen, und hat dann der Reihe nach eine m_1^{te}, m_2^{te}, m_3^{te}, ... Wurzel aus je einem Ausdrucke auszuziehen, welcher durch die vorherig bekannten Grössen rational ausdrückbar ist.

§ 174. Wir können die Lösung noch auf eine andere Art bewerkstelligen.

Es sei $m=m_1.m_2\ldots m_\omega=m_1.n_1=m_2n_2=\ldots=m_\omega n_\omega$; dann kann man, wie gezeigt ist, folgende Gleichungen aufstellen:

A_1) $g_1(x)=0$, mit den Wurzeln x_1, $\theta^{m_1}(x_1)$, $\theta^{2m_1}(x_1)$, ... $\theta^{(n_1-1)m_1}(x_1)$, deren Koefficienten rationale Funktionen einer Resolvente $\chi_1=x_1+\theta^{m_1}(x_1)+\ldots$ sind; χ_1 ist die Wurzel einer Gleichung m_1^{ten} Grades $h_1(\chi)=0$.

A_2) $g_2(x)=0$, mit den Wurzeln x_1, $\theta^{m_2}(x_1)$, $\theta^{2m_2}(x_1)$, ... $\theta^{(n_2-1)m_2}(x_1)$, deren Koefficienten rationale Funktionen einer Resolvente $\chi_2=x_1+\theta^{m_2}(x_1)+\ldots$ sind; χ_2 ist die Wurzel einer Gleichung m_2^{ten} Grades $h_2(\chi)=0$.

. . . . . .

A_ω) $g_3(x)=0$, mit den Wurzeln x_1, $\theta^{m_\omega}(x_1)$, $\theta^{2m_\omega}(x_1)$, ... $\theta^{(n_\omega-1)m_\omega}(x_1)$, deren Koefficienten rationale Funktionen einer Resolvente $\chi_\omega=x_1+\theta^{m_\omega}(x_1)+\ldots$ sind; χ_ω ist die Wurzel einer Gleichung m_ω^{ten} Grades $h_\omega(\chi)=0$.

Wählen wir nun m_1, m_2, ... m_ω so, dass sie zu einander relativ prim sind, dann haben

$$g_1(x)=0,\ g_2(x)=0,\ \ldots\ g_\omega(x)=0$$

nur die eine Wurzel x_1 mit einander gemeinsam. Diese kann also mittels der Methode des grössten gemeinsamen Teilers rational durch die Koefficienten von g_1, g_2, ... g_ω d. h. durch die Koefficienten von $f(x)$ und durch χ_1, χ_2, ... χ_ω ausgedrückt werden.

Die Auflösung von $f(x)=0$ hängt sonach von der Kenntnis je einer Wurzel der Gleichungen

$$h_1(\chi)=0,\ h_2(\chi)=0,\ \ldots\ h_\omega(\chi)=0$$

der Grade m_1, m_2, ... m_ω ab. Hat man

$$m=p_1^{\alpha_1}.p_2^{\alpha_2}.\ \ldots\ p_\omega^{\alpha_\omega},$$

wo p_1, p_2, ... p_ω die verschiedenen Primfaktoren von m bezeichnen, so ist

$$m_1=p_1^{\alpha_1},\ m_2=p_2^{\alpha_2},\ \ldots\ m_\omega=p_\omega^{\alpha_\omega}$$

zu wählen. Falls für eine der Gleichungen $h_\lambda(\chi)=0$ der Exponent α_λ grösser als 1 wird, muss man zur früheren Methode der Lösung zurückgreifen, um ein χ_λ zu bestimmen.

§ 175. Um für die soeben behandelten Gleichungen ein Beispiel zu bilden, nehmen wir

$$\theta(x) = \frac{\alpha_1 x + \beta_1}{\gamma_1 x + \delta_1} = \frac{\alpha x + \beta}{\gamma x + \delta}$$

und bezeichnen weiter

$$\theta^2(x) = \frac{\alpha_2 x + \beta_2}{\gamma_2 x + \delta_2}, \quad \theta^3(x) = \frac{\alpha_3 x + \beta_3}{\gamma_3 x + \delta_3}, \ \cdots \ \theta^m(x) = \frac{\alpha_m x + \beta_m}{\gamma_m x + \delta_m}.$$

Da aber auch

$$\theta^m(x) = \frac{\alpha_{m-1}(\alpha_1 x + \beta_1) + \beta_{m-1}(\gamma_1 x + \delta_1)}{\gamma_{m-1}(\alpha_1 x + \beta_1) + \delta_{m-1}(\gamma_1 x + \delta_1)}$$

ist, so ergiebt die Vergleichung beider Ausdrücke

$$\alpha_m = \alpha_1 \alpha_{m-1} + \gamma_1 \beta_{m-1}, \quad \beta_m = \beta_1 \alpha_{m-1} + \delta_1 \beta_{m-1},$$
$$\gamma_m = \alpha_1 \gamma_{m-1} + \gamma_1 \delta_{m-1}, \quad \delta_m = \beta_1 \gamma_{m-1} + \delta_1 \delta_{m-1}.$$

Aus ihnen kann man sofort die Gleichungen erlangen

$$7) \quad \alpha_m \delta_m - \beta_m \gamma_m = (\alpha_1 \delta_1 - \beta_1 \gamma_1)(\alpha_{m-1} \delta_{m-1} - \beta_{m-1} \gamma_{m-1})$$
$$= (\alpha_1 \delta_1 - \beta_1 \gamma_1)^2 (\alpha_{m-2} \delta_{m-2} - \beta_{m-2} \gamma_{m-2}) = \cdots$$
$$= (\alpha \delta - \beta \gamma)^m.$$

Wir suchen jetzt die Bedingungen dafür auf, dass

$$\theta^m(x) = x$$

wird. Zuerst bereiten wir jedoch durch Division mit

$$\sqrt{\alpha\delta - \beta\gamma} \quad \text{respektive} \quad \sqrt{\beta\gamma - \alpha\delta},$$

jenachdem $\alpha\delta - \beta\gamma$ positiv oder negativ ist, die Koefficienten so zu, dass

$$8) \qquad \alpha\delta - \beta\gamma = \pm 1$$

wird. Null kann die Grösse $\alpha\delta - \beta\gamma$ nicht sein, weil sonst

$$\theta(x) = \frac{\beta}{\delta} = \frac{\alpha}{\gamma}$$

würde. Ferner berechnen wir diejenigen Werte x', x'', welche durch θ ungeändert bleiben, bei denen also

$$x = \frac{\alpha x + \beta}{\gamma x + \delta},$$
$$\gamma x^2 + (\delta - \alpha) x - \beta = 0$$

ist. Es findet sich, jenachdem $\alpha\delta - \beta\gamma = +1$ oder $= -1$ ist,

$$\gamma x' = \frac{\alpha - \delta}{2} + \sqrt{\left(\frac{\alpha + \delta}{2}\right)^2 \mp 1}, \quad \gamma x'' = \frac{\alpha - \delta}{2} - \sqrt{\left(\frac{\alpha + \delta}{2}\right)^2 \mp 1}$$

und daher

$$\frac{\gamma x' - \alpha}{\gamma x'' - \alpha} = \pm \left[\frac{\alpha + \delta}{2} - \sqrt{\left(\frac{\alpha + \delta}{2}\right)^2 \mp 1}\right]^2 = N.$$

A) Wir setzen voraus, dass x' von x'' verschieden, also N nicht gleich Eins sei. Dann wird

$$\frac{\theta(x)-x'}{\theta(x)-x''}=N\cdot\frac{x-x'}{x-x''},\quad \frac{\theta^2(x)-x'}{\theta^2(x)-x''}=N^2\cdot\frac{x-x'}{x-x''},\ \cdots$$

$$\frac{\theta^m(x)-x'}{\theta^m(x)-x''}=N^m\cdot\frac{x-x'}{x-x''};$$

$N^m=1$ ist daher notwendige Bedingung dafür, dass $\theta^m x=x$ wird; diese Bedingung ist auch hinreichend, denn aus ihr folgt

$$\frac{\theta^m(x)}{x'-x''}=\frac{x}{x'-x''}$$

und, da x' von x'' verschieden ist, auch

$$\theta^m(x)=x.$$

Die Bedingung $N^m=1$ oder

$$(\pm 1)^m\left[\frac{\alpha+\delta}{2}-\sqrt{\left(\frac{\alpha+\delta}{2}\right)^2\mp 1}\right]^{2m}=1$$

kann durch komplexe oder durch reelle Werte der Klammer erfüllt werden.

Im ersteren Falle werden die oberen Vorzeichen gelten; ausserdem wird

$$\left(\frac{\alpha+\delta}{2}\right)^2<1$$

sein, so dass wir setzen können

$$\frac{\alpha+\delta}{2}=\cos\frac{\lambda\pi}{\mu},$$

$$N^m=\left(\cos\frac{\lambda\pi}{\mu}-i\sin\frac{\lambda\pi}{\mu}\right)^{2m}=\cos\frac{2\lambda m\pi}{\mu}-i\sin\frac{2\lambda m\pi}{\mu}.$$

Es muss sonach, wenn λ, μ keinen gemeinsamen Teiler haben, $\mu=m$ sein; d. h. es wird

$$9)\qquad \frac{\alpha+\delta}{2}=\cos\frac{\lambda\pi}{m},$$

wo λ eine beliebige zu m teilerfremde ganze Zahl ist. Ist also 9) erfüllt, so wird aus der Reihe x, $\theta(x)$, $\theta^2(x)$, ... die Funktion $\theta^m(x)$ die erste sein, welche den Anfangswert x liefert.

Wenn die Klammer reell ist, so kann sie nur die Werte -1, $+1$ annehmen, falls eine ihrer Potenzen gleich Eins werden soll. Die Annahme $N=+1$ würde auf $x'=x''$ führen, was ausgeschlossen ist. Die Annahme $N=-1$ liefert

$$\alpha+\delta=0,\quad \alpha^2+\beta\gamma=1,$$

$\theta^2(x)=x$, was wegen $m=2$ mit der Bedingung 9) übereinstimmt.

B) Es ist nur noch $x' = x''$ zu betrachten. Hierfür erhält man

$$\left(\frac{\alpha+\delta}{2}\right)^2 \mp 1 = 0;$$

folglich muss das obere Vorzeichen gelten und es wird:

I) $\alpha+\delta = \pm 2.$ II) $\alpha\delta - \beta\gamma = +1.$

Diese beiden Voraussetzungen ergeben leicht:

$$\theta^2(x) = \frac{(2\alpha \mp 1)x + 2\beta}{2\gamma x + (2\delta \mp 1)},$$

$$\theta^3(x) = \frac{(3\alpha \mp 2)x + 3\beta}{3\gamma x + (3\delta \mp 2)},$$

. . . . . .

$$\theta^m(x) = \frac{[m\alpha \mp (m-1)]x + m\beta}{m\gamma x + [m\delta \mp (m-1)]}.$$

Soll nun $\theta^m(x) = x$ sein, so würde aus der Gleichsetzung folgen

$$\gamma x^2 + (\delta - \alpha)x - \beta = 0,$$

d. h. es müsste schon $\theta(x) = x$ sein. Ausserdem erkennt man, dass die θ^m sich mit wachsendem m asymptotisch dem Werte nähern

$$\theta^\infty(x) = \frac{(\alpha \mp 1)x + \beta}{\gamma x + (\delta \mp 1)}.$$

Es hat sich somit gezeigt, dass

$$\alpha + \delta = 2\cos\frac{\lambda\pi}{m}, \quad \alpha\delta - \beta\gamma = 1$$

die notwendigen und hinreichenden Bedingungen dafür sind, dass

$$\theta^m(x)$$

die erste der Funktionen $\theta^\mu(x)$ wird, welche den Wert x wieder annimmt. Dabei muss λ relativ prim zu m sein. Für $m = 2$ fällt die zweite Bedingung fort.

---

§ 176. Wir haben in § 171 die Gleichung ν^{ten} Grades 6) aufgestellt, welcher

$$\varphi_1 = x_1 + \theta(x_1) + \theta^2(x_1) + \ldots + \theta^{m-1}(x_1),$$
$$\varphi_2 = x_2 + \theta(x_2) + \theta^2(x_2) + \ldots + \theta^{m-1}(x_2),$$
. . . . . .

als Wurzeln zugehören. Diese Gleichung ist ohne besondere weitere Voraussetzungen eine allgemeine und daher, wie wir später sehen werden, nicht lösbar. Wenn diese Gleichung 6) jedoch dieselben Eigenschaften hätte, wie 1) sie besass, so würde die in den ersten Paragraphen dieses Kapitels angegebene Methode, durch welche wir

von 1) auf 6) gelangten, in ihrer Verwendung auf 6) eine neue Reduktion dieser Gleichung hervorrufen.

Die erste Eigentümlichkeit von 1) bestand in ihrer Irreduktibilität. Wir zeigen:

Lehrsatz IX. Die Gleichung, welche $\varphi_1, \varphi_2, \ldots \varphi_\nu$ zu Wurzeln hat, ist irreduktibel.

Wäre dies nicht der Fall, so wäre die Gruppe von

$$6) \qquad \varphi^\nu - S_1 \cdot \varphi^{\nu-1} + S_2 \varphi^{\nu-2} - \ldots \pm S_\nu = 0$$

intransitiv. Die transitive, imprimitive Gruppe von 1) besteht aus Substitutionen von der symbolischen Form

$$t = \sigma_\alpha \cdot s_1^{\gamma_1} s_2^{\gamma_2} \ldots s_\nu^{\gamma_\nu},$$

wobei σ_α nur die $\varphi_1, \varphi_2, \ldots \varphi_\nu$ versetzt, wobei ferner

$$s_\alpha = [x_\alpha \theta(x_\alpha) \theta^2(x_\alpha) \ldots \theta^{m-1}(x_\alpha)]$$

ist und der Ausdruck der Substitution t im Sinne von § 73 aufzufassen ist. Die σ_α (nicht mehr symbolisch genommen) bilden die Gruppe von 6); wäre sie intransitiv, so würde wegen der Form von t dasselbe mit der Gruppe von 1) stattfinden, d. h. es wäre gegen die Voraussetzung 1) reduktibel nach § 154.

§ 177. Die zweite Eigentümlichkeit von 1) bestand darin, dass eine ihrer Wurzeln x'_1 durch eine andere x_1 rational ausdrückbar war. Daraus folgte, dass für $x'_1 = \theta(x_1)$

$$x_1, \quad \theta(x_1), \quad \theta^2(x), \ldots \theta^{m-1}(x_1)$$

ebenfalls Wurzeln von 1) werden, und dass wegen

$$x_1 = \theta^m(x_1) = \theta^{m-1}(x'_1)$$

auch x_1 rational durch x'_1 ausdrückbar wird.

Es wäre nun eine scharfumgrenzte, berechtigte Aufgabe, unter den x solche weitere Beziehungen aufzusuchen und festzusetzen, dass auch bei 6) eine Wurzel φ_2 rational in φ_1 darstellbar wird, und die Gleichung gilt:

$$\varphi_2 = \tau(\varphi_1).$$

Die allgemeinen Bedingungen hierfür sind aber wohl nicht in übersichtliche Form zu bringen.

Wir behandeln daher statt der allgemeinen Frage nur denjenigen Spezialfall, in welchem aus einer rationalen Beziehung, die zwischen φ_α und φ_β besteht, auch eine solche zwischen x_α und x_β folgt, d. h. es soll

$$R) \qquad x_\beta = \text{Rat.}(x_\alpha) \quad \text{aus} \quad \varphi_\beta = \text{Rat.}_1(\varphi_\alpha)$$

sich ergeben. Dieser Fall kann völlig erledigt werden. Notwendig ist aber die in R) enthaltene Voraussetzung nicht. Dies zeige folgendes Beispiel. Es seien

$$x_1, \qquad x_2, \qquad \cdots \qquad x_5;$$

$$\theta(x_1) = \frac{x_1}{x_1 - 1}, \quad \theta(x_2) = \frac{x_2}{x_2 - 1}, \cdots \theta(x_5) = \frac{x_5}{x_5 - 1} \qquad [\theta^2(x) = x]$$

die Wurzeln einer Gleichung zehnten Grades; dann wird

$$\varphi_1 = x_1 + \theta(x_1) = \frac{x_1^2}{x_1 - 1}, \quad \varphi_2 = x_2 + \theta(x_2) = \frac{x_2^2}{x_2 - 1}.$$

Setzen wir nun fest, dass

$$\varphi_2 = \frac{1}{-\varphi_1 + 2\cos\frac{\pi}{5}} \quad \text{oder} \quad \frac{x_2^2}{x_2 - 1} = \frac{x_1 - 1}{-x_1^2 + 2\cos\frac{\pi}{5}(x_1 - 1)}$$

wird, so ist den geforderten Bedingungen genügt; zwischen den Grössen φ_1, φ_2 besteht die Beziehung $\varphi_2 = \text{Rat.}_1 \varphi_1$, aber aus dieser Beziehung zwischen φ_1 und φ_2 kann keine rationale Beziehung $x_2 = \text{Rat.}\, x_1$ abgeleitet werden.

Wir nehmen also R) als giltig an. Da nun

$$\varphi_2 = \tau(\varphi_1)$$

sein soll, so erlaubt dies einen Rückschluss auf

$$x_2 = \theta_1(x_1);$$

es gelten demnach für 1) die beiden Beziehungen

$$x'_1 = \theta(x_1), \quad x_2 = \theta_1(x_1);$$

also wird, da 6) dieselben Verhältnisse aufweisen soll,

$$\varphi_2 = \tau(\varphi_1), \quad \varphi_3 = \tau_1(\varphi_1).$$

Daraus folgt dann wieder

$$x_3 = \theta_2(x_1)$$

u. s. w.; d. h. alle Wurzeln von 1) sind rationale Funktionen einer unter ihnen; nur dann kann bei 6) das Gleiche stattfinden. Demnach haben wir zu setzen:

$A_1)$ $x'_1 = \theta(x_1), \quad x_2 = \theta_1(x_1), \quad x_3 = \theta_2(x_1), \ldots x_\nu = \theta_{\nu-1}(x_1),$

$B_1)$ $\varphi_2 = \tau(\varphi_1), \quad \varphi_3 = \tau_1(\varphi_1), \quad \varphi_4 = \tau_2(\varphi_1), \ldots \varphi_\nu = \tau_{\nu-2}(\varphi_1).$

Die Existenz der Beziehungen $A_1)$ ist für die Erfüllung der Forderungen $B_1)$ notwendig, aber noch nicht hinreichend. Damit

$$\varphi_2 = \tau(\varphi_1)$$

sei, muss φ_2 bei der Anwendung der Substitutionen ungeändert bleiben, welche φ_1 nicht ändern, also bei der Einsetzung von $\theta(x_1)$ statt x_1. Wir haben

$$\varphi_2 = x_2 + \theta(x_2) + \theta^2(x_2) + \ldots = \theta_1(x_1) + \theta\theta_1(x_1) + \theta^2\theta_1(x_1) + \ldots$$

Jede symmetrische Funktion der Grössen x_2, $\theta(x_2)$, $\theta^2(x_2)$, ... ist durch φ_2 rational ausdrückbar und umgekehrt; bleibt daher φ_2 bei der Einsetzung von $\theta(x_1)$ statt x_1 ungeändert, so findet dies bei jeder symmetrischen Funktion S der m Grössen x_2, $\theta(x_2)$, ... statt. Es ist demnach

$$S[\theta_1(x_1), \theta\theta_1(x_1), \theta^2\theta_1(x_1), \ldots] = S[\theta_1\theta(x_1), \theta\theta_1\theta(x_1), \theta^2\theta_1\theta(x_1), \ldots].$$

Insbesondere müssen die Koefficienten der Gleichung, welche die Wurzeln

$$\theta_1(x_1), \quad \theta\theta_1(x_1), \quad \theta^2\theta_1(x_1), \ldots \theta^{m-1}\theta_1(x_1)$$

hat, mit den entsprechenden derjenigen Gleichung übereinstimmen, der die Wurzeln

$$\theta_1\theta(x_1), \quad \theta\theta_1\theta(x_1), \quad \theta^2\theta_1\theta(x_1), \ldots \theta^{m-1}\theta_1\theta(x_1)$$

zugehören. Beide Reihen stimmen daher in ihren Elementen überein, und es wird

$$\theta_1\theta(x_1) = \theta^{\alpha_1}\theta_1(x_1)$$

werden. Dies ist notwendig, damit $\varphi_2 = \tau(\varphi_1)$ sei; es ist hierfür auch hinreichend. Denn unter dieser Voraussetzung wird

$$\theta_1\theta(x_1) + \theta\theta_1\theta(x_1) + \theta^2\theta_1\theta(x_1) + \ldots = \theta^{\alpha_1}\theta_1(x_1) + \theta^{\alpha_1+1}\theta_1(x_1) + \ldots + \theta^{\alpha_1-1}\theta_1(x_1)$$
$$= \theta_1(x_1) + \theta\theta_1(x_1) + \theta^2\theta_1(x_1) + \ldots = \varphi_2,$$

so dass φ_2 wirklich bei der Substitution von $\theta(x_1)$ statt x_1 ungeändert bleibt. Da mit φ_3, φ_4, ... φ_ν dasselbe stattfindet, so erhalten wir die Reihe von Bedingungen

$$A_2) \quad \theta_1\theta(x_1) = \theta^{\alpha_1}\theta_1(x_1), \quad \theta_2\theta(x_1) = \theta^{\alpha_2}\theta_2(x_1), \quad \theta_3\theta(x_1) = \theta^{\alpha_3}\theta_3(x_1) \ldots$$

und wissen, dass die Erfüllung von A_1) und A_2) notwendig und hinreichend dafür ist, dass die Gleichungen B_1) auftreten.

Damit ist die Frage aber noch nicht abgeschlossen, denn die Gleichung 6) soll, um die Reduktion bis zu Ende zuzulassen, dieselben Spezialitäten besitzen wie 1). Wir müssen also A_2) in eine neue Forderungsreihe für 6) übertragen:

$$B_2) \qquad \tau_1\tau(\varphi_1) = \tau^{\beta_1}\tau_1(\varphi_1), \quad \tau_2\tau(\varphi_1) = \tau^{\beta_2}\tau_2(\varphi_1), \ldots;$$

somit werden den Wurzeln x_1, x'_1, ... von 1) neue Bedingungen auferlegt werden müssen. Es ist

$$\varphi_2 = \tau(\varphi_1) = x_2 + \theta(x_2) + \ldots = \theta_1(x_1) + \theta\theta_1(x_1) + \ldots,$$
$$\varphi_3 = \tau_1(\varphi_1) = x_3 + \theta(x_3) + \ldots = \theta_2(x_1) + \theta\theta_2(x_1) + \ldots$$

Verwandelt man also in dem Ausdrucke

$$\varphi_1 = x_1 + \theta(x_1) + \theta^2(x_1) + \ldots$$

x_1 in $\theta_1(x_1)$, so geht φ_1 in $\tau(\varphi_1)$, und verwandelt man x_1 in $\theta_2(x_1)$, so geht φ_1 in $\tau_1(\varphi_1)$ über. Führt man dies in den beiden obigen Gleichungen durch, so entsteht

$$\tau_1\tau(\varphi_1) = \theta_2\theta_1(x_1) + \theta\theta_2\theta_1(x_1) + \theta^2\theta_2\theta_1(x_1) + \ldots,$$
$$\tau^2(\varphi_1) = \tau\tau(\varphi_1) = \theta_1{}^2(x_1) + \theta\theta_1{}^2(x_1) + \theta^2\theta_1{}^2(x_1) + \ldots,$$
$$\tau^{\beta_1}(\varphi_1) = \theta_1{}^{\beta_1}(x_1) + \theta\theta_1{}^{\beta_1}(x_1) + \theta^2\theta_1{}^{\beta_1}(x_1) + \ldots,$$
$$\tau^{\beta_1}\tau_1(\varphi_1) = \theta_1{}^{\beta_1}\theta_2(x_1) + \theta\theta_1{}^{\beta_1}\theta_2(x_1) + \theta^2\theta_1{}^{\beta_1}\theta_2(x_1) + \ldots$$

Infolge von B_2) muss also sein

$$\theta_2\theta_1(x_1) + \theta\theta_2\theta_1(x_1) + \ldots = \theta_1{}^{\beta_1}\theta_2(x_1) + \theta\theta_1{}^{\beta_1}\theta_2(x_1) + \ldots$$

Wir werden die Gleichheit der einzelnen Glieder links und rechts nachweisen. Unter S verstehen wir eine beliebige symmetrische Funktion von m Grössen und setzen:

$$\psi_1 = S[x_1, \theta(x_1), \theta^2(x_1), \ldots],$$
$$\psi_2 = S[x_2, \theta(x_2), \theta^2(x_2), \ldots] = S[\theta_1(x_1), \theta\theta_1(x_1), \ldots],$$
$$\psi_3 = S[x_3, \theta(x_3), \theta^2(x_3), \ldots] = S[\theta_2(x_1), \theta\theta_2(x_1), \ldots].$$

Dann gehören ψ_1 und φ_1 zu derselben Gruppe; ebenso ψ_2 und φ_2 zu einer und derselben und auch ψ_3 und φ_3. Da aber φ_2, φ_3 rational in φ_1 sind und umgekehrt, wie sich aus dem ersten Teile dieses Paragraphen für die Grössen x_1 und x'_1 ergab (S. 199), so werden φ_1, φ_2, φ_3 zu derselben Gruppe gehören; folglich ist dies auch bei ψ_1, ψ_2, ψ_3 der Fall, und wir erhalten die Gleichungen, in denen das Argument x_1 unterdrückt ist,

$$\psi_2 = \omega(\psi_1), \quad \psi_3 = \omega_1(\psi_1),$$
$$\psi_1 = \chi(\varphi_1), \quad \psi_2 = \psi_1(\theta_1) = \chi(\varphi_2) = \chi\varphi_1(\theta_1), \quad \psi_3 = \chi(\varphi_3).$$

Verwandelt man in der Gleichung

$$\psi_3 = \omega_1(\psi_1) = \chi(\varphi_3) = \chi\tau_1(\varphi_1)$$

x_1 in x_2 und damit φ_1 in $\varphi_2 = \tau(\varphi_1)$, ψ_1 in $\psi_2 = \omega(\psi_1)$, so entsteht

$$\omega_1\omega(\psi_1) = \chi[\tau_1\tau(\varphi_1)].$$

Ebenso erhält man durch geeignete Substitutionen

$$\omega^{\beta_1}\omega_1(\psi_1) = \chi[\tau^{\beta_1}\tau_1(\varphi_1)],$$

so dass aus der Gleichheit der rechten Seiten dieser beiden letzten Gleichungen, welche gemäss B_2) bestehen soll, der Schluss zu ziehen ist, dass

$$\omega_1\omega(\psi_1) = \omega^{\beta_1}\omega_1(\psi_1)$$

sein wird. Geht man auf die Bedeutung der ω zurück, so folgt, dass

$$S[\theta_2\,\theta_1(x_1), \theta\,\theta_2\,\theta_1(x_1), \theta^2\,\theta_2\,\theta_1(x_1), \ldots\,\theta^{m-1}\,\theta_2\,\theta_1(x_1)]$$
$$= S[\theta_1{}^{\beta_1}\theta_2(x_1), \theta\theta_1{}^{\beta_1}\theta_2(x_1), \theta^2\theta_1{}^{\beta_1}\theta_2(x_1), \ldots\,\theta^{m-1}\theta_1{}^{\beta_1}\theta_2(x_1)]$$

ist. Nimmt man für S die elementaren symmetrischen Funktionen, so folgt auch genau wie oben die Übereinstimmung der Elementenreihe

$$\theta_2\theta_1(x_1), \quad \theta\theta_2\theta_1(x_1), \quad \theta^2\theta_2\theta_1(x_1), \ldots \theta^{m-1}\theta_2\theta_1(x_1)$$

mit

$$\theta_1^{\beta_1}\theta_2(x_1), \quad \theta\theta_1^{\beta_1}\theta_1(x_1), \quad \theta^2\theta_1^{\beta_1}\theta_2(x_1), \ldots \theta^{m-1}\theta_1^{\beta_1}\theta_2(x),$$

abgesehen von der Aufeinanderfolge. Insbesondere erhält man

$$\theta_2\theta_1(x_1) = \theta^{\gamma_2}\theta_1^{\beta_1}\theta_2(x_1).$$

Diese Bedingung reicht für die in B_2) geforderte Gleichung aus, denn man hat

$$\tau_1\tau(\varphi_1) = \tau^{\beta_1}\tau_1(\varphi_1)$$

$$\tau_1\tau(\varphi_1) = \theta_2\,\theta_1(x_1) + \theta\,\theta_2\,\theta_1(x_1) + \theta^2\,\theta_2\,\theta_1(x_1) + \ldots,$$
$$\tau^{\beta_1}\tau_1(\varphi_1) = \theta_1^{\beta_1}\theta_2(x_1) + \theta\theta_1^{\beta_1}\theta_2(x_1) + \theta^2\theta_1^{\beta_1}\theta_2(x_1) + \ldots$$

Es sind also die Gleichungen

$$A_3) \qquad \theta_2\theta_1(x_1) = \theta^{\gamma_2}\theta_1^{\beta_2}\theta_2(x), \quad \theta_3\theta_1(x) = \theta^{\gamma_3}\theta_1^{\beta_3}\theta_3(x_1), \ldots$$

notwendig und hinreichend, um die Gleichungen B_2) nach sich zu ziehen.

Die Übertragung der durch A_3) für die Wurzeln von 1) ausgesprochenen Eigenschaften auf die Wurzeln von 6) giebt zu einer neuen Forderungsreihe Anlass

$$B_3) \qquad \tau_2\tau_1(\varphi_1) = \tau^{\varepsilon_2}\tau_1^{\delta_2}\tau_2(\varphi_1), \quad \tau_3\tau_1(\varphi_1) = \tau^{\varepsilon_3}\tau_1^{\delta_3}\tau_3(\varphi_1), \ldots$$

und an diese knüpft sich das weitere Raisonnement in derselben Weise an, wie oben an B_2). Die Ableitungen und die Resultate wiederholen sich und man sieht:

Lehrsatz X. Damit die Gleichung 6), von welcher die Resolvente φ_1 abhängt, dieselben Wurzelbeziehungen besitze und also dieselben Reduktionen erlaube, wie die ursprüngliche Gleichung 1), ist es hinreichend [und unter der Voraussetzung R) auch notwendig], dass man für die Wurzeln von 1) habe:

$$A_1) \qquad x_1, \quad \theta(x_1), \quad \theta_1(x_1), \quad \theta_2(x_1), \ldots,$$
$$A_2) \qquad \theta_1\theta(x_1) = \theta^{\alpha_1}\theta_1(x_1), \quad \theta_2\theta(x_1) = \theta^{\alpha_2}\theta_2(x_1), \ldots,$$
$$A_3) \qquad \theta_2\theta_1(x_1) = \theta^{\beta_2}\theta_1^{\gamma_2}\theta_2(x_1), \quad \theta_3\theta_1(x_1) = \theta^{\beta_3}\theta_1^{\gamma_3}\theta_3(x_1), \ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

§ 178. Wir stellen die Gruppe einer so definierten Gleichung her.

Da die Gleichung 1) irreduktibel ist, so wird die Gruppe derselben transitiv sein. Da alle ihre Wurzeln durch eine unter ihnen rational darstellbar sind, so ist ihr Grad gleich ihrer Ordnung (§ 154).

Wegen der Transitivität giebt es Substitutionen

$$s, s_1, s_2, \ldots, \text{ welche } x_1 \text{ in } \theta(x_1), \theta_1(x_1), \theta_2(x_1), \ldots$$

umwandeln. Dann werden die Produkte

$$s_1 . s, \quad s_2 . s, \ldots; \quad s_2 . s_1, \quad s_3 . s_1, \ldots; \ldots$$

das Element x_1 in

$$\theta_1 \theta(x_1), \quad \theta_2 \theta(x_1), \ldots; \quad \theta_2 \theta_1(x_1), \quad \theta_3 \theta_1(x_1), \ldots; \ldots$$

und die Produkte

$$s^{\alpha_1} s_1, \quad s^{\alpha_2} s_2, \ldots; \quad s^{\beta_2} s_1^{\gamma_2} s_2, \quad s^{\beta_2} s_1^{\gamma_3} s_3, \ldots; \ldots$$

werden dasselbe Element x_1 in

$$\theta^{\alpha_1} \theta_1(x_1), \quad \theta^{\alpha_2} \theta_2(x_1), \ldots; \quad \theta^{\beta_2} \theta_1^{\gamma_2} \theta_2(x_1), \quad \theta^{\beta_3} \theta_1^{\gamma_3} \theta_3(x_1), \ldots; \ldots$$

umsetzen; wegen der Bedingungen A_2), A_3), ... üben also

$s_1 s$ und $s^{\alpha_1} s_1$, $s_2 s$ und $s^{\alpha_2} s_2, \ldots$; $s_2 s_1$ und $s^{\beta_2} s_1^{\gamma_2} s_2$, $s_3 s_1$ und $s^{\beta_3} s^{\gamma_3} s, \ldots$

auf x_1 denselben Einfluss aus. Bei den Gruppen Ω, mit denen wir es hier zu thun haben, bestimmt die Umsetzung eines Elementes bereits die gesamte Substitution (§ 90); daher ist

$\mathcal{A}_2$) $\qquad s_1 s = s^{\alpha_1} s_1, \quad s_2 s = s^{\alpha_2} s_2, \ldots$

$\mathcal{A}_3$) $\qquad s_2 s_1 = s^{\beta_2} s_1^{\gamma_2} s_2, \quad s_3 s_1 = s^{\beta_3} s_1^{\gamma_3} s_3, \ldots$

. . . .

Umgekehrt kann man aus der Transitivität schliessen, dass die Gleichung irreduktibel sei; aus dem Umstande, dass ihr Grad ihrer Ordnung gleich ist, folgt die Eigenschaft der rationalen Darstellbarkeit aller Wurzeln durch eine einzige; aus den Beziehungen $\mathcal{A}_2$), $\mathcal{A}_3$), ... lassen sich die Beziehungen A_2), A_3) ableiten.

Als Beispiele für solche Gruppen mögen folgende beiden dienen:

I) $\quad s = (x_0 x_1 x_2 x_3)(x_4 x_5 x_6 x_7), \quad s_1 = (x_0 x_4)(x_1 x_7)(x_2 x_6)(x_3 x_5)$;

zwischen diesen Substitutionen herrscht die Beziehung

$$s_1 s = s^3 s_1.$$

II) Es sei p eine Primzahl, a gehöre zum Exponenten r (mod. p); dann geben

$$s_1 = (x_{1,0}, x_{1,1}, \ldots x_{1,p-1})(x_{2,0}, x_{2,1}, \ldots x_{2,p-1}) \ldots (x_{r,0}, x_{r,1}, \ldots x_{r,p-1}),$$
$$s_2 = (x_{1,0}, x_{2,0}, \ldots x_{r,0})(x_{1,1}, x_{2,a}, \ldots x_{r,a^{r-1}}) \ldots$$
$$\ldots (x_{1,p-1}, x_{2,(p-1)a}, \ldots x_{r,(p-1)a^{r-1}})$$

eine Gruppe von der verlangten Beschaffenheit. Es wird nämlich

$s_2 s_1$ die Wurzel $x_{m,n}$ in $x_{m+1, an+1}$,

$s_1^{\alpha_1} s_2$ „ „ $x_{m,n}$ „ $x_{m+1, an+a\alpha_1}$

umwandeln. Bestimmt man demnach α_1 durch die Kongruenz

$$a \alpha_1 \equiv 1 \quad (\text{mod. } p),$$

so ist

$$s_2 s_1 = s_1^{\alpha_1} s_2.$$

§ 179. Wir stellen jetzt folgende Definition auf:*

Definition. Sind alle Wurzeln einer Gleichung rationale Funktionen einer einzigen x_1, und sind die rationalen Beziehungen derart, dass, wenn

$$x_1, \quad \theta_1(x_1), \quad \theta_2(x_1), \ldots \theta_{n-1}(x_1)$$

die n Wurzeln bedeuten, dann die Gleichungen

$$\theta_\alpha\theta_\beta(x_1) = \theta_\beta\theta_\alpha(x_1)$$

bestehen, so heisst die Gleichung eine „Abel'sche Gleichung".

Es folgt nun weiter:

Lehrsatz XI. Abel'sche Gleichungen sind algebraisch auflösbar.**

Wie wir sehen, bilden die Abel'schen Gleichungen, abgesehen von der im vorigen Lehrsatze X) vorausgesetzten Irreduktibilität, einen Spezialfall der dort behandelten Gleichungen. Sobald daher nachgewiesen ist, dass jeder irreduktible Faktor einer Abel'schen Gleichung, gleich Null gesetzt, wiederum eine Abel'sche Gleichung liefert, haben wir die Richtigkeit des neuen Lehrsatzes dargethan. Es seien

$$f_1(x), \quad f_2(x)$$

zwei irreduktible Faktoren des Polynoms der vorgelegten Abel'schen Gleichung; der erste möge, gleich Null gesetzt,

R) $$x_1, \quad \theta_1(x_1), \quad \theta_2(x_1), \ldots \theta_{r-1}(x_1)$$

als Wurzeln besitzen, während $\vartheta(x_1)$ eine Wurzel des zweiten sei. Dann liefert der erste von beiden Faktoren, gleich Null gesetzt, sicher eine irreduktible Abel'sche Gleichung. Nun haben

$$f_1(x) = 0, \quad f_2[\vartheta(x)] = 0$$

eine Wurzel gemeinsam, nämlich x_1; folglich hat $f_2(x)$ auch zu Wurzeln

R') $$\vartheta(x_1), \quad \vartheta[\theta_1(x_1)], \quad \vartheta[\theta_2(x_1)], \ldots \vartheta[\theta_{r-1}(x_1)],$$

und diese gehen, wenn man die Gleichungen der Voraussetzung anwendet, in

R'') $$\vartheta(x_1), \quad \theta_1[\vartheta(x_1)], \quad \theta_2[\vartheta(x_1)], \ldots \theta_{r-1}[\vartheta(x_1)]$$

über. Alle diese Wurzeln sind demnach rationale Funktionen der einen $\vartheta(x_1)$. Für diese gilt ferner, ebenfalls nach den Gleichungen der Voraussetzung

$$\theta_\alpha\theta_\beta[\vartheta(x_1)] = \theta_\beta\vartheta[\theta_\alpha(x_1)] = \theta_\beta\theta_\alpha[\vartheta(x_1)].$$

---

* C. Jordan: Traité etc., § 402.

** Abel: Oeuvres complètes, I, Nr. XI; p. 114—140.

Es ist nur noch zu zeigen, dass die Elemente der Reihe R′) auch alle Wurzeln von $f_2(x) = 0$ erschöpfen. Jedenfalls bleibt eine symmetrische Funktion der Elemente von R″) oder R′) für alle Substitutionen ungeändert, welche die symmetrischen Funktionen der Elemente von R) nicht ändern. Die ersteren Funktionen sind also durch eine der letzteren rational darstellbar. Mit den Koefficienten von $f_1(x)$ sind demnach auch die von

10) $\{x - \vartheta(x_1)\}\{x - \theta_1[\vartheta(x_1)]\} \ldots \{x - \theta_{r-1}[\vartheta(x_1)]\} = 0$

bekannt. Da $f_2(x)$ irreduktibel ist, so liefert 10) wirklich alle Wurzeln von $f_2(x) = 0$; diese sind also sämtlich in R′) enthalten. Ob 10) irreduktibel ist, kann wegen der Unbestimmtheit von ϑ nicht behauptet werden.

Es zerfällt also die Abel'sche Gleichung in irreduktible Abel'sche Gleichungen, deren Grade sämtlich gleich demjenigen oder Teiler desjenigen Grades sind, der zur Gleichung $f_1(x_1) = 0$ gehört.

§ 180. Aus der Definition Abel'scher Gleichungen und den Resultaten von § 178 folgt, dass die Substitutionen s, s_1, s_2, ..., einer irreduktiblen Abel'schen Gleichung eine transitive Gruppe von gegeneinander vertauschbaren Substitutionen bilden, und dass umgekehrt durch eine transitive Gruppe mit vertauschbaren Substitutionen eine irreduktible Abel'sche Gleichung charakterisiert wird.

Ersichtlich ist ferner, dass, wenn G die Gruppe einer irreduktiblen Abel'schen Gleichung ist, und wenn Γ derart isomorph zu G angenommen wird, dass jeder Substitution von G nur eine Substitution von Γ entspricht, dass dann auch Γ die Gruppe einer Abel'schen Gleichung werden wird. Denn entsprechen die Substitutionen s_α, s_β von G den Substitutionen σ_α, σ_β von Γ, so werden

$$s_\alpha s^\beta \text{ und } \sigma_\alpha\sigma_\beta, \quad s_\beta s_\alpha \text{ und } \sigma_\beta\sigma_\alpha$$

einander entsprechen. Da ferner $s_\alpha s_\beta = s_\beta s_\alpha$ ist, und da zu jedem s nur ein σ gehört, so wird

$$\sigma_\alpha\sigma_\beta = \sigma_\beta\sigma_\alpha.$$

Folglich ist Γ die Gruppe einer Abel'schen Gleichung.

§ 181. Das System sämtlicher Wurzeln einer Abel'schen Gleichung erfüllt die Voraussetzungen, welche in den Untersuchungen von §§ 131—133 gemacht wurden.

Man kann sie daher in folgendes System bringen:

$$\theta_1^{h_1}\theta_2^{h_2}\theta_3^{h_3}\ldots\theta_k^{h_k}(x_1) \qquad (h_i = 0, 1, 2, \ldots n_i - 1),$$
$$n_1 n_2 n_3 \ldots n_k = n,$$

worin jede Wurzel ein, aber auch nur ein Mal dargestellt wird. Die Zahlen n_1, n_2, ... n_k sind so beschaffen, dass eine jede derselben durch

die folgende teilbar oder ihr gleich wird, und dass es die kleinsten sind, welche respektive

$$\theta_1^{n_1}(x_1) = x_1, \quad \theta_2^{n_2}(x) = x_1, \ \ldots \ \theta_k^{n_k}(x_1) = x_1$$

liefern. Bezeichnet man diejenige Substitution der Gruppe unserer Abel'schen Gleichung, welche x_1 in $\theta_\alpha(x_1)$ umwandelt, durch s_α, so ist s_α eine eindeutig bestimmte Substitution. Es können dann die Substitutionen der Gruppe gleichfalls in ein System gebracht werden

$$s_1^{h_1} s_2^{h_2} s_3^{h_3} \ldots s_k^{h_k} \quad (h_i = 0, 1, 2, \ldots n_i - 1),$$
$$n_1 n_2 n_3 \ldots n_k = n,$$

wo jede Substitution ein und auch nur ein Mal dargestellt wird und, entsprechend den Eigenschaften der θ, auch

$$s_1^{n_1} = 1, \quad s_2^{n_2} = 1, \ \ldots \ s_k^{n_k} = 1$$

sein muss. Die Zahlen n_1, n_2, $\ldots$ n_k sind dieselben, welche oben bei den θ auftraten.

Wir nehmen nun, um eine Resolvente zu bilden,

$$\psi_1(x_1) = \sum_{h_2, h_3, \ldots h_k} \theta_2^{h_2} \theta_3^{h_3} \ldots \theta_k^{h_k}(x_1) \qquad (h_i = 0, 1, \ldots n_i - 1),$$

und stellen eine cyklische Funktion auf, in welcher ω_1 eine primitive n_1^{te} Einheitswurzel bedeuten soll,

$$\chi_1(x_1) = [\psi_1(x_1) + \omega_1 \theta_1 \psi_1(x_1) + \omega_1^2 \theta_1^2 \psi_1(x_1) + \ldots + \omega_1^{n_1-1} \theta_1^{n_1-1} \psi_1(x_1)]^{n_1}.$$

Dann bleibt $\chi_1(x_1)$ für die Gruppe der Gleichung ungeändert. Denn für die Substitutionen der Untergruppe

$$G_2) \qquad G_2 = \{s_2, s_3, \ldots s_k\}$$

ändert sich $\psi_1(x_1)$ nicht; für die Potenzen von s_1 geht $\psi_1(x_1)$ respektive in

$$\theta_1 \psi_1(x_1), \quad \theta_1^2 \psi_1(x_1), \ \ldots \ \theta_1^{n_1-1} \psi_1(x_1)$$

über, was auf den Wert von χ_1 keinen Einfluss hat. Folglich ist χ_1 durch die Koefficienten der gegebenen Abel'schen Gleichung und durch ω_1 rational darstellbar. ψ_1 ist demgemäss nach Lehrsatz IV) als Wurzel einer „einfachsten" Abel'schen Gleichung darstellbar. Mit ψ_1 sind alle Funktionen bekannt, die zu der Untergruppe G_2 von G gehören.

Setzt man weiter

$$\psi_{1,2}(x_1) = \sum_{h_3, \ldots h_k} \theta_3^{h_3} \theta_4^{h_4} \ldots \theta_k^{h_k}(x_1) \quad (h_i = 0, 1, 2, \ldots n_i - 1),$$

und bildet man die cyklische Resolvente

$$\chi_{1,2}(x_1) =$$
$$[\psi_{1,2}(x_1) + \omega_2 \theta_2 \psi_{1,2}(x_1) + \omega_2^2 \theta_2^2 \psi_{1,2}(x_1) + \ldots + \omega_2^{n_2-1} \theta_2^{n_2-1} \psi_{1,2}(x_1)]^{n_2},$$

in welcher ω_2 eine primitive n_2^{te} Einheitswurzel bedeuten soll, dann bleibt die Funktion $\chi_{1,2}$ für die Gruppe G_2 ungeändert, und ist also rational durch ψ_1 darstellbar. Denn für die Substitution der Gruppe

G_3) $$G_3 = \{s_3, s_4, \ldots s_k\}$$

bleibt $\psi_{1,2}$ ungeändert und die Potenzen von s_2 rufen nur die Werte

$$\theta_2\psi_{1,2},\ \theta_2^{\,2}\psi_{1,2},\ \ldots\ \theta_2^{\,n_2-1}\psi_{1,2}$$

hervor. Man kommt daher durch die Anwendung des Lehrsatzes IV) von ψ_1 auf $\psi_{1,2}$ durch die Auflösung einer „einfachsten" Abel'schen Gleichung des Grades n_2.

Allgemein können wir, wenn

$$\psi_{1,2,\ldots\nu} = \sum_{h_\nu+1\ldots h_k} \theta_{\nu+1}^{\,h_\nu+1}\ldots\theta_k^{h_k}(x_1)$$

und, unter Einführung der primitiven n_ν^{ten} Einheitswurzel ω_ν,

$$\chi_{1,2,\ldots\nu} =$$
$$[\psi_{1,2,\ldots\nu} + \omega_\nu\theta_\nu\psi_{1,2,\ldots\nu} + \omega_\nu^{\,2}\theta_\nu^{\,2}\psi_{1,2,\ldots\nu} + \ldots + \omega_\nu^{\,n_\nu-1}\theta_\nu^{\,n_\nu-1}\psi_{1,2,\ldots\nu}]^{n_\nu}$$

gesetzt wird, die Berechnung von $\psi_{1,2,\ldots\nu}$ auf diejenige einer ähnlich gebildeten Funktion

$$\psi_{1,2,\ldots\nu-1} = \sum_{h_\nu\ldots h_k} \theta_\nu^{h_\nu}\ldots\theta_k^{h_k}(x_1)$$

mit Hilfe einer solchen „einfachsten" Abel'schen Gleichung zurückführen, wie sie im Lehrsatz IV) definiert werden.

Man erkennt daher durch die Fortsetzung dieses Verfahrens:

Lehrsatz XI. Ordnen sich die n Wurzeln einer Abel'schen Gleichung in das System

$$\theta_1^{h_1}\theta_2^{h_2}\ldots\theta_k^{h_k}(x_1) \qquad (h_i = 0,\ 1,\ 2,\ \ldots\ n_{i-1})$$
$$n_1 . n_2 . n_3 \ldots n_k = n,$$

so kann man die Lösung derselben durch diejenige von k „einfachsten" Abel'schen Gleichungen von den Graden

$$n_1,\ n_2,\ n_3,\ \ldots\ n_k$$

bewirken.*

§ 181. Die Behandlung irreduktibler Abel'scher Gleichungen kann noch nach einer anderen Methode durchgeführt werden, zu deren Auseinandersetzung wir jetzt übergehen:

Lehrsatz XII. Die Lösung einer irreduktiblen Abel'schen Gleichung vom Grade $n = p_1^{\alpha_1}p_2^{\alpha_2}\ldots$, wo $p_1, p_2, \ldots$ die verschie-

---

* L. Kronecker: Berl. Ber. Nachtrag z. Dezemberheft 1877, p. 846—851.

denen Primzahlteiler von n bedeuten, kann auf die von irreduktiblen Abel'schen Gleichungen der Grade $p_1^{\alpha_1}$, $p_2^{\alpha_2}$, ... reduziert werden.

Den Beweis* knüpfen wir an die Betrachtungen der Gruppeneigenschaften; der Einfachheit halber nehmen wir $n = p_1^{\alpha_1} p_2^{\alpha_2}$ an.

Da auch die Ordnung der Gruppe $r = n$ ist, so ist die Ordnung jeder ihrer Substitutionen ein Teiler von n, also von der Form $p_1^{a_1} p_2^{a_2}$; eine jede Substitution kann demnach aus einer Kombination ihrer $p_2^{a_2\text{ten}}$ Potenz (welche die Ordnung $p_1^{b_1}$ hat) und ihrer $p_1^{a_1\text{ten}}$ Potenz (welche die Ordnung $p_2^{b_2}$ hat) zusammengesetzt werden. Folglich erhält man alle Substitutionen der Gruppe G, wenn man alle diejenigen

$$t'_1,\ t'_2,\ t'_3 \ldots t'_{r_1},$$

deren Ordnung eine Potenz von p_1 ist, mit allen denjenigen

$$t''_1,\ t''_2,\ t''_3,\ \ldots\ t''_{r_2}$$

kombiniert, deren Ordnung eine Potenz von p_2 ist. Alle Substitutionen von G haben somit, da alle t unter einander vertauschbar sind, die Form

$$s = (t'_\alpha t'_\beta t'_\gamma \ldots)\,(t''_\delta t''_\varepsilon t''_\vartheta \ldots).$$

Die Ordnung des Produkts in der ersten Klammer ist eine Potenz von p_1. Denn es wird

$$t'^{p_1^{\alpha_1}}_\alpha t'^{p_1^{\alpha_1}}_\beta \ldots = (t'_\alpha t_\beta \ldots)^{p_1^{\alpha_1}} = 1$$

werden, so dass die Ordnung der Klammergrösse ein Teiler von $p_1^{\alpha_1}$ ist. Zwei Substitutionen

$$(t'_\alpha t'_\beta \ldots)\,(t''_\delta t''_\varepsilon \ldots) \quad \text{und} \quad (t'_a t'_b \ldots)\,(t''_d t''_e \ldots)$$

sind von einander verschieden, wenn nicht die beiden Klammern entsprechend gleich sind. Denn aus der angenommenen Gleichheit folgt

$$(t'_\alpha t'_\beta \ldots)\,(t'_a t'_b \ldots)^{-1} = (t''_\delta t''_\varepsilon \ldots)^{-1}\,(t''_d t''_e \ldots),$$

und da die Ordnung der linken Seite ein Teiler von $p_1^{\alpha_1}$, die der rechten Seite ein Teiler von $p_2^{\alpha_2}$ ist, so muss dieser Teiler gleich 1 sein; daraus folgt das Behauptete.

Die Anzahl der Substitutionen s ist gleich $n = p_1^{\alpha_1} p_2^{\alpha_2}$. Da nun die Substitutionen t' eine Gruppe bilden und da jede Substitution der Gruppe als Ordnung $p_1^{\alpha_1}$ hat, so wird die Ordnung der Gruppe selbst $p_1^{m_1}$ zu setzen sein (§ 43). Ebenso wird die Ordnung der aus den t'' gebildeten Gruppe gleich $p_2^{m_2}$. Dann folgt aus

---

* C. Jordan: Traité etc. §§ 405 – 407.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} = p_1^{m_1} p_2^{m_2},$$

dass $m_1 = \alpha_1$, $m_2 = \alpha_2$ ist.

Es sei nun φ eine zur Gruppe der t'' gehörige Funktion; dann hat sie $p_1^{\alpha_1}$ Werte und hängt von einer Gleichung des Grades $p_1^{\alpha_1}$ ab, deren Gruppe durch die t' gebildet wird oder, wenn man will, durch eine aus den Werten von φ als Elementen gebildeten Gruppe, welche der Gruppe der t' isomorph ist (vergl. §§ 156 und 180). Diese Gleichung ist demnach eine Abel'sche.

Ebenso hängt die zur Gruppe der t' gehörige Funktion ψ von einer Abel'schen Gleichung des Grades $p_2^{\alpha_2}$ ab.

Denkt man sich φ und ψ berechnet, so wird

$$\chi = \alpha' \varphi + \beta' \psi$$

zur Gruppe 1 gehören. Durch χ sind also alle rationalen Wurzelfunktionen rational darstellbar; speziell sind es die Wurzeln selbst. Damit ist der Satz bewiesen.

§ 182. Lehrsatz XIII. Die Auflösung einer irreduktibeln Abel'schen Gleichung vom Grade p^α kann auf die Lösung einer Reihe Abel'scher Gleichungen zurückgeführt werden, deren Gruppen nur Substitutionen der Ordnung p und der Ordnung 1 enthalten.

Es sei G die Gruppe einer solchen Gleichung. Die Ordnung einer jeden Substitution von G ist eine Potenz von p. Es möge p^λ die Ordnung derjenigen Substitutionen sein, deren Ordnung ein Maximum ist. Dann bilden diejenigen Substitutionen von G, deren Ordnung nur bis $p^{\lambda-1}$ aufsteigt, eine Gruppe H. Denn, wenn t_1, t_2 zwei von diesen Substitutionen sind, so wird wegen der Vertauschbarkeit

$$(t_1 t_2)^{p^{\lambda-1}} = t_1^{p^{\lambda-1}} t_2^{p^{\lambda-1}} = 1$$

werden, so dass $t_1 t_2$ dieselbe Eigenschaft besitzt, wie t_1 und t_2 einzeln.

Es möge jetzt φ eine zu H gehörige Funktion sein; wenn p^α die Ordnung von H ist, wird φ eine $p^{\alpha-a}$-wertige Funktion sein und demnach von einer Gleichung des Grades $p^{\alpha-a}$ abhängen. Wendet man auf φ eine Substitution τ von G an, die nicht auch in H enthalten ist, so wird φ hierfür nur p Werte annehmen, weil τ^p in H vorkommt. Die Substitutionen unter den Werten von φ, welche durch G entstehen und welche eine zu G einstufig isomorphe Gruppe bilden (§ 156), haben deshalb sämtlich die Ordnung p. Man kann, wie im vorigen Paragraphen, aus dem Isomorphismus den Schluss ziehen, dass die Gleichung, zu der φ gehört, eine Abel'sche Gleichung ist, denn ihre Gruppe ist die soeben konstruierte, die zwischen den φ besteht.

Kennt man φ, so reduziert sich die Gruppe G der gegebenen Abel'schen Gleichung auf H. Wir bezeichnen mit H_1 die Gruppe derjenigen Substitutionen von H, deren Ordnung den Grad $p^{\lambda-2}$ nicht überschreitet, mit φ_1 eine zugehörige Funktion, und erkennen dann wieder, dass φ_1 aus φ durch eine Abel'sche Gleichung vom Grade $p^{\alpha-a_1}$ gefunden werden kann, deren Gruppe nur Substitutionen von der Ordnung p enthält u. s. f.

§ 183. Lehrsatz XIV. Die Auflösung einer irreduktiblen Abel'schen Gleichung vom Grade p^α, deren Gruppe nur Substitutionen der Ordnung p und der Ordnung 1 enthält, lässt sich auf diejenige von α irreduktiblen Abel'schen Gleichungen des Grades p zurückführen.

Obgleich dieser Satz, als Spezialfall des in § 180 abgeleiteten, schon bewiesen ist, wollen wir ihn dennoch mit Hilfe der zuletzt benutzten Methode nochmals verifizieren.

Sei s_1 eine Substitution der Gruppe G der vorgelegten Abel'schen Gleichung; dann ist die Ordnung von s_1 gleich p; ferner sei s_2 eine nicht unter $s_1, s_1^2, \ldots s_1^{p-1}, 1$ enthaltene neue Substitution von G. Dann ist $s_1 . s_2 = s_2 . s_1$; demnach enthält die aus s_1 und s_2 gebildete Gruppe $H_2 = \{s_1, s_2\}$ höchstens p^2 Substitutionen. Sie enthält auch wirklich so viele, falls aus $s_1^a s_2^b = s_1^\alpha s_2^\beta$ die Gleichheiten $a = \alpha$, $b = \beta$ sich ergeben. Wäre $s_1^a s_2^b = s_1^\alpha s_2^\beta$, so wäre auch $s_2^{\beta-b} = s_1^{a-\alpha}$. Für jedes von 0 verschiedene $\beta - b$ kann man eine Zahl m so bestimmen, dass

$$m(\beta - b) \equiv 1 \pmod{p.}$$

wird. Man erhält daher

$$s_2 = s_2^{m(\beta-b)} = s_1^{m(a-\alpha)}.$$

Dies ist unmöglich. Also musste $\beta = b$ und $\alpha = a$ sein.

Ist $\alpha > 2$, so sei s_3 eine nicht unter den p^2 Substitutionen der Form $s_1^a s_2^b$ enthaltene neue Substitution. Da $s_1 s_3 = s_3 s_1$, $s_2 s_3 = s_3 s_2$, so enthält $H_3 = \{s_1, s_2, s_3\}$ höchstens n^3 Substitutionen. Sie enthält auch wirklich so viele, falls aus $s_1^a s_2^b s_3^c = s_1^\alpha s_2^\beta s_3^\gamma$ die Gleichheiten $a = \alpha$, $b = \beta$, $c = \gamma$ sich ergeben. Es würde aus jener Gleichung folgen $s_3^{\gamma-c} = s_1^{a-\alpha} s_2^{b-\beta}$ u. s. w. ganz wie oben.

Geht man in dieser Art weiter fort, so erkennt man, dass alle p^α Substitutionen in die Form

$$s_1^{\lambda_1} s_2^{\lambda_2} \ldots s_\alpha^{\lambda_\alpha} \quad (\lambda_i = 0, 1, \ldots p-1)$$

gebracht werden können, wobei eine jede ein und auch nur ein Mal auftritt (vergl. § 180). Wählt man nun zu Resolventen

$$\varphi_\alpha \quad (x_1, x_2, \ldots x_n) \quad \text{zu} \quad H'_\alpha = \{s_1, s_2, \ldots s_{\alpha-1}\},$$
$$\varphi_{\alpha-1}(x_1, x_2, \ldots x_n) \quad \text{„} \quad H'_{\alpha-1} = \{s_1, s_2, \ldots s_{\alpha-2}, s_\alpha\},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\varphi_1 \quad (x_1, x_2, \ldots x_n) \quad \text{zu} \quad H'_1 = \{s_2, s_3, \ldots s_\alpha\}$$

gehörig, so hängt jede derselben von einer Abel'schen Gleichung des Grades p ab. Die Wurzeln der gegebenen Gleichung des Grades p^α sind durch $\varphi_1, \varphi_2, \ldots \varphi_\alpha$ rational darstellbar, da zu

$$\psi = \beta_1\varphi_1 + \beta_2\varphi_2 + \ldots + \beta_\alpha\varphi_\alpha$$

die Gruppe 1 gehört (vergl. § 174).

§ 184. Die p^α Wurzeln einer derartigen Gleichung können durch

$$x_{z_1, z_2, \ldots z_\alpha} \qquad (z_\lambda = 0, 1, 2, \ldots p-1)$$

bezeichnet werden. Es sei $x_{\zeta_1, \zeta_2, \ldots \zeta_\alpha}$ die Wurzel, welche $s_1^{\zeta_1} s_2^{\zeta_2} \ldots s_\alpha^{\zeta_\alpha}$ auf $x_{z_1, z_2, \ldots z_\alpha}$ folgen lässt. Dann wird

$$s_1^{\zeta_1} s_2^{\zeta_2} \ldots s_\alpha^{\zeta_\alpha} \cdot s_1^{\xi_1} s_2^{\xi_2} \ldots s_\alpha^{\xi_\alpha} = s_1^{\zeta_1+\xi_1} s_2^{\zeta_2+\xi_2} \ldots s_\alpha^{\zeta_\alpha+\xi_\alpha}$$

(wegen der linken Seite) auf $x_{z_1, z_2, \ldots z_\alpha}$ diejenige Wurzel folgen lassen, durch welche $s_1^{\xi_1} \ldots s_\alpha^{\xi_\alpha}$ die Wurzel $x_{\zeta_1, \zeta_2, \ldots \zeta_\alpha}$ ersetzt; wegen der rechten Seite ist dies $x_{\zeta_1+\xi_1, \zeta_2+\xi_2, \ldots \zeta_\alpha+\xi_\alpha}$; folglich ersetzt die beliebige Substitution $s_1^{\xi_1} s_2^{\xi_2} \ldots s_\alpha^{\xi_\alpha}$ das beliebige Element

$$x_{\zeta_1, \zeta_2, \ldots \zeta_\alpha} \quad \text{durch} \quad x_{\zeta_1+\xi_1, \zeta_2+\xi_2, \zeta_\alpha+\xi_\alpha},$$

d. h. man erhält in der analytischen Darstellungsweise der Substitutionen

$$s_1^{k_1} s_2^{k_2} \ldots s_\alpha^{k_\alpha} = |z_1, z_2, \ldots z_\alpha \quad z_1+k_1, z_2+k_2, \ldots z_\alpha+k_\alpha| \pmod p.$$

Die Gruppe einer Abel'schen Gleichung vom Grade p^α, deren Substitutionen sämtlich die Ordnung p besitzen, wird durch die arithmetischen Substitutionen des Grades p^α (mod. p) gebildet.

§ 185. Wir wollen endlich den Übergang von den Untersuchungen dieses Kapitels zu den spezielleren Fragen des vorhergehenden machen.

Wir verstehen unter n eine beliebige ganze Zahl und unter a den Quotienten $\frac{2\pi}{n}$, dann genügen bekanntlich die n Grössen

$$\cos a, \cos 2a, \cos 3a, \ldots \cos na$$

einer Gleichung, deren Koefficienten rationale Zahlen sind. Diese Gleichung lautet:

$$C) \qquad x^n - \tfrac{1}{4} n x^{n-2} + \tfrac{1}{16} \frac{n(n-3)}{1.2} x^{n-4} - \ldots = 0.$$

Setzen wir $x = \cos a$, so wird für ein beliebiges ganzes m

$$\cos m\,a = \theta(\cos a),$$

wobei θ eine ganze Funktion bezeichnet. Versteht man ebenso unter $\theta_1(\cos a)$ den Wert $\cos m_1 a$, so erhält man, wenn man in der vorigen Gleichung $m_1 a$ statt des Argumentes a einsetzt, die Gleichung

$$\cos(m \,.\, m_1 a) = \theta(\cos m_1 a) = \theta\theta_1 \cos a.$$

Ebenso findet man, wenn in $\theta_1 \cos a = \cos m_1 a$ das Argument a durch ma ersetzt wird, das Resultat

$$\cos(m_1 \,.\, ma) = \theta_1(\cos m a) = \theta_1\theta \cos a.$$

Folglich findet für die Wurzeln von C) die Beziehung statt, dass alle durch eine einzige unter ihnen rational ausdrückbar sind und dass

$$\theta_1\theta(x_1) = \theta\theta_1(x_1) \quad (x_1 = \cos a)$$

wird. Die Gleichung C) ist also eine Abel'sche Gleichung. Daher kann man

$$x_1 = \cos a = \cos\frac{2\pi}{n}$$

algebraisch bestimmen. Wir haben hier ein Beispiel für § 179.

§ 186. Es sei jetzt n eine ungerade Primzahl $n = 2\nu + 1$, dann werden die Wurzeln der Gleichung C) folgende sein:

$$\cos\frac{2\pi}{2\nu+1},\quad \cos\frac{4\pi}{2\nu+1},\quad \cdots\quad \cos\frac{4\nu\pi}{2\nu+1},\quad \cos 2\pi.$$

Da hier die letzte Wurzel $= 1$ ist, so ist die Gleichung C) durch $x-1$ teilbar. Die anderen Wurzeln werden einander paarweise gleich, nämlich

$$\cos\frac{2m\pi}{2\nu+1} = \cos\frac{(2\nu+1-m)\,2\pi}{2\nu+1}.$$

Folglich kann man eine Gleichung mit rationalen Koefficienten aus C) ableiten, deren Wurzeln die folgenden sein werden:

$$\cos\frac{2\pi}{2\nu+1},\quad \cos\frac{4\pi}{2\nu+1},\quad \cdots\quad \cos\frac{2\nu\pi}{2\nu+1}.$$

Diese Gleichung hat die Form

$$C_1)\quad x^\nu + \tfrac{1}{2}x^{\nu-1} - \tfrac{1}{4}(\nu-1)x^{\nu-2} - \tfrac{1}{8}(\nu-2)x^{\nu-3} + \tfrac{1}{16}\frac{(\nu-2)(\nu-3)}{1.2}x^{\nu-4}$$
$$+ \tfrac{1}{32}\frac{(\nu-3)(\nu-4)}{1.2}x^{\nu-5} - \ldots = 0$$

Wir führen nun folgende Bezeichnung ein:

$$\cos\frac{2\pi}{2\nu+1} = \cos a = x;$$

dann hat man nach dem Obigen

$$\cos\frac{2m\pi}{2\nu+1} = \theta(x) = \cos ma,$$

so dass der Gleichung C_1) auch durch die Wurzeln

$$\theta(x),\quad \theta^2(x),\quad \theta^3(x),\ \ldots$$

genügt wird. Da für jeden Wert von a die Beziehung herrscht

$$\cos ma = \theta(\cos a),$$

so folgt hieraus der Reihe nach

$$\theta^2(\cos a) = \cos m^2 a,\quad \theta^3(\cos a) = \cos m^3 a,\ \ldots$$
$$\theta^\mu(\cos a) = \cos m^\mu a,\ \ldots$$

und die Wurzeln x, $\theta(x)$, $\theta^2(x)$, ... treten unter der Form auf

$$\cos a,\quad \cos ma,\quad \cos m^2 a,\quad \cos m^3 a,\ \ldots\ \cos m^\mu a,\ \ldots$$

Verstehen wir nun unter g irgend eine primitive Wurzel mod. $(2\nu+1)$, so werden die ν Glieder der Reihe

R_1) $\qquad \cos a,\quad \cos ga,\quad \cos g^2 a,\ \ldots\ \cos g^{\nu-1}.a$

von einander verschieden sein. Denn aus der Gleichung

$$\cos g^\alpha a = \cos g^\beta a,\quad \alpha > \beta,$$

in welcher α und β kleiner als ν sind, würde folgen

$$g^\alpha a = \pm g^\beta a + 2k\pi,$$

und wenn man für a seinen Wert $\dfrac{2\pi}{2\nu+1}$ einsetzt,

$$g^\alpha = \pm g^\beta + k(2\nu+1),$$
$$g^\alpha \mp g^\beta = g^\beta(g^{\,-\beta} \mp 1) = k(2\nu+1).$$

Dividieren wir diese Gleichung durch g^β und multiplizieren mit $g^{\alpha-\beta} \pm 1$, so finden wir hieraus die Kongruenz

$$g^{2(\alpha-\beta)} \equiv 1 \mod (2\nu+1).$$

Weil jedoch $2(\alpha-\beta) < 2\nu$ ist, so ist diese Kongruenz unmöglich. Infolgedessen muss $\cos g^\alpha a$ von $\cos g^\beta a$ verschieden sein.

Ferner ist

$$\cos g^\nu a = \cos a;$$

denn man hat $g^{2\nu} - 1 = (g^\nu - 1)(g^\nu + 1)$ gleich einem Vielfachen von $2\nu+1$; also ist einer der beiden Faktoren durch die Primzahl $2\nu+1$ teilbar und für eins der beiden Vorzeichen gilt die Gleichung

$$g^\nu = \pm 1 + k(2n+1),$$

und somit ergiebt sich auch die Beziehung

$$\cos g^\nu a = \cos[\pm 1 + k.(2\nu+1)]a = \cos(\pm a + 2\pi k) = \cos a.$$

Hieraus erkennt man, dass die ν Wurzeln der Gleichung C_1) durch die Reihe R_1) oder durch

$$x,\quad \theta(x),\quad \theta^2(x),\ \ldots \theta^{\nu-1}(x)$$

geliefert werden, während $\theta^\nu(x) = x$ wird. Die Gleichung C_1) ist also algebraisch lösbar. Wir haben hier ein Beispiel für § 172.

Setzt man $\nu = n_1 . n_2 . \ldots . n_\omega$, so kann man den Kreisumfang in $2\nu + 1$ gleiche Teile teilen durch die Lösung von ω Gleichungen der Grade $n_1, n_2, \ldots n_\omega$. Sind $n_1, n_2, \ldots n_\omega$ zu einander prim, so sind die Koefficienten dieser Gleichungen rationale Zahlen (§ 173).

Ist $\nu = 2^\omega$, so erhält man den Satz über die Konstruktion regulärer Polygone, mit Hilfe von Zirkel und Lineal.

Zwölftes Kapitel.

Gleichungen, bei denen rationale Beziehungen zwischen drei Wurzeln bestehen.

§ 187. Nach der Behandlung einiger Gleichungen, bei denen alle Wurzeln rationale Funktionen einer einzigen sind, liegt es nahe, solche Gleichungen zu untersuchen, bei denen alle Wurzeln rationale Funktionen von zweien unter ihnen sind. Wir betrachten nur irreduktible Gleichungen dieser Art. Es sei

$$x_3 = \varphi_3(x_1, x_2),\quad x_4 = \varphi_4(x_1, x_2),\ \ldots\ x_n = \varphi_n(x_1, x_2);$$

dann wird eine Substitution, welche die beiden Elemente x_1, x_2 ungeändert lässt, überhaupt kein Element ändern.

Ist s_α eine beliebige Substitution der Gruppe der Gleichung, und s'_α eine andere, welche x_1, x_2 in derselben Weise versetzt, wie s_α es thut, so wird $s'_\alpha . s_\alpha^{-1}$ weder x_1 noch x_2 bewegen, also gleich 1 sein; d. h. es wird $s'_\alpha = s_\alpha$.

Sind $s_1, s_2, \ldots s_r$ alle Substitutionen der Gruppe G, so können wir eine Tabelle entwerfen, in deren erster Zeile

$$s_1,\ s_2,\ s_3,\ \ldots\ s_r$$

stehen. Nun giebt es $n(n-1)$ verschiedene Möglichkeiten der Umsetzung von x_1, x_2 unter den n Elementen $x_1, x_2, \ldots x_n$. Ist eine dieser Umsetzungen in jener ersten Zeile noch nicht vertreten, d. h. ist $r < n(n-1)$, so sei t_2 eine beliebige Substitution, welche diese neue Umsetzung hervorruft. Dann werden

$$t_2 s_1,\quad t_2 s_2,\quad t_2 s_3,\ \ldots\ t_2 s_r$$

Umsetzungen von x_1, x_2 liefern, die sämtlich von einander verschieden sind und von denen keine auch der ersten Zeile angehört. Ist $2 . r$

noch $< n(n-1)$, so giebt es eine neue Umsetzung von x_1, x_2, die in keiner der beiden Zeilen vorkommt. Wir bilden eine beliebige Substitution t_3, welche diese Umsetzung liefert, und konstruieren

$$t_3 s_1, \quad t_3 s_2, \quad t_3 s_3, \ldots t_3 s_r$$

als dritte Zeile unserer Tabelle u. s. w., bis alle $n(n-1)$ Möglichkeiten erschöpft sind. Daraus sieht man:

Lehrsatz I. Die Ordnung der Gruppe einer irreduktiblen Gleichung n^{ten} Grades, bei der alle Wurzeln durch zwei unter ihnen rational darstellbar sind, ist ein Teiler von $n(n-1)$.

§ 188. Wir fügen zu den bisherigen Annahmen über unsere Gleichung

1) $$f(x) = 0$$

noch die hinzu, dass ihr Grad gleich einer Primzahl sein soll.

Definition. Eine irreduktible Gleichung eines Primzahlgrades, deren Wurzeln sämtlich durch zwei unter ihnen rational ausdrückbar sind, heisst eine Galois'sche Gleichung.*

Es sei p der Grad von $f(x)$; dann wird die Ordnung der Gruppe ein Teiler von $p(p-1)$ sein. Da $f(x) = 0$ irreduktibel ist, so ist G_1, die Gruppe von 1), transitiv; deshalb ist ihre Ordnung durch p teilbar, und G enthält (§ 48) eine Substitution der Ordnung p. Es sei dies s. Käme ausser den Potenzen von s in G noch eine Substitution t der Ordnung p vor, so würden alle $s^\alpha t^\beta$ von einander verschieden sein. Denn aus

$$s^\alpha t^\beta = s^a t^b$$

würde folgen

$$s^{-a+\alpha} = t^{b-\beta};$$

und wenn man, was stets möglich ist, r durch die Kongruenz

$$r(b-\beta) \equiv 1 \pmod{p} \qquad (\beta \not\equiv b)$$

bestimmt, so folgt aus der vorigen Gleichung durch Erhebung in die r^{te} Potenz

$$t = s^{(\alpha-a)r}.$$

Es wäre also, was ausgeschlossen werden muss, t eine Potenz von s. Demnach bildeten die $s^\alpha t^\beta$ bereits p^2 von einander verschiedene Substitutionen, während die Ordnung von G nur ein Teiler von $p(p-1)$ sein sollte. Es können also in G ausser den Potenzen von s keine Substitutionen der Ordnung p vorkommen.

Wir untersuchen, ob G noch andere Substitutionen enthält, welche alle Elemente umsetzen. Transformiert man eine Substitution p^{ter}

* Ev. Galois: Oeuvres mathématiques, herausgegeben von Liouville im 11. Bande des Journal de mathématiques pures et appliquées, 1846; p. 381—444.

Ordnung s durch irgend eine Substitution σ von G, so wird s sich in eine seiner Potenzen umwandeln müssen; es wird also

$$\sigma^{-1} s \sigma = s^{\lambda}.$$

Angenommen, es führt σ das Element x_1 in x_α über, dann wird σ das Element x_2 in $x_{\alpha+\lambda}$, x_3 in $x_{\alpha+2\lambda}$, ... x_β in $x_{\alpha+(\beta-1)\lambda}$ überführen. Dabei bleibt aber in σ das Element x_γ, für welches

$$\gamma \equiv \alpha + (\gamma - 1)\lambda \pmod{p},$$
$$\gamma \equiv \frac{\lambda - \alpha}{\lambda - 1} \pmod{p}$$

wird, ungeändert. Es könnte also höchstens für $\lambda = 1$ ein σ existieren, welches alle Elemente umsetzt. Hierfür wäre dann x_1 in x_α, x_2 in $x_{\alpha+1}$, x_3 in $x_{\alpha+2}$, ... übergeführt. Daher erhielte man

$$\sigma = (x_1 x_\alpha x_{2\alpha-1} x_{3\alpha-2} \ldots x_{n\alpha-(n-1)} \ldots) \ldots$$

Der erste Cyklus schliesst sich nach $x_{n\alpha-(n-1)}$, wenn

$$(n+1)\alpha - n \equiv n(\alpha - 1) + \alpha \equiv 1 \pmod{p},$$
$$n \equiv -1 \equiv p - 1 \pmod{p}$$

ist. σ würde somit eine cyklische Substitution der Ordnung p werden, und das ist nicht möglich, wenn es nicht eine Potenz von s wird. Es folgt daher, dass es ausser

$$s, s^2, s^3, \ldots s^{p-1},$$

keine Substitution in G giebt, die alle Elemente umsetzt; demnach giebt es in G auch keine Substitution, ausser der Einheit, welche mehr als ein Element ungeändert lässt (§ 63). Wir sehen also:

Lehrsatz II. Die Gruppe einer Galois'schen Gleichung enthält ausser der Substitution 1 nur noch $p-1$ Substitutionen der Ordnung p und Substitutionen, welche $p-1$ Elemente umsetzen.

Diese Gruppe haben wir in den §§ 125 flgg. studiert. Die dort erlangten Resultate können wir uns hier zu Nutze machen.

§ 189. Es sei eine Substitution p^{ter} Ordnung in G

$$s = (x_1 x_2 x_3 \ldots x_p);$$

wir bilden die Resolvente

$$\varphi_1 = (x_1 + \omega^\alpha x_2 + \omega^{2\alpha} x_3 + \ldots + \omega^{(p-1)\alpha} x_p)^p,$$

in welcher ω eine primitive p^{te} Einheitswurzel bedeutet; φ_1 bleibt für s und seine Potenzen, also für eine Gruppe der Ordnung p ungeändert. Ist die Ordnung der Gruppe der vorgelegten Galois'schen Gleichung

$p\frac{p-1}{\sigma}$, so hat φ_1 gerade $\frac{p-1}{\sigma}$ Werte (§ 43), welche sämtlich zu derselben Gruppe gehören (§ 126), so dass

$$\varphi_2 = \chi_2(\varphi_1), \quad \varphi_3 = \chi_3(\varphi_1), \quad \varphi_{\frac{p-1}{\sigma}} = \chi_{\frac{p-1}{\sigma}}(\varphi_1)$$

wird. Da ferner die Substitutionen, die zwischen $\varphi_1, \varphi_2, \ldots$ bestehen, mit einander vertauschbar sind (§ 128), so ist auch

$$\chi_\alpha \chi_\beta(\varphi_1) = \chi_\beta \chi_\alpha(\varphi_1).$$

Die Gleichung $\frac{p-1}{\sigma}^{\text{ten}}$ Grades, von welcher φ_1 abhängt, ist demnach eine Abel'sche. Ist diese gelöst, so hängen $x_1, x_2, \ldots x_p$ von einer zweiten Abel'schen Gleichung des Grades p ab, deren Koefficienten rational in φ_1 sind und deren Gruppe aus den Potenzen von s besteht.

Lehrsatz III. Die Auflösung einer Galois'schen Gleichung, deren Gruppe die Ordnung $p\frac{p-1}{\sigma}$ besitzt, kann auf diejenige zweier Abel'schen Gleichungen der Grade p und $\frac{p-1}{\sigma}$ reduziert werden. Ist $\frac{p-1}{\sigma}$ eine zusammengesetzte Zahl, so kann die letztere Gleichung in andere Abel'sche Gleichungen niederer Grade zerfällt werden.

§ 190. Als einfachstes Beispiel einer Galois'schen Gleichung bietet sich die binomische Gleichung des Primzahlgrades p

$$x^p - A = 0$$

dar, falls die reelle p^{te} Wurzel des absoluten Wertes der reellen Grösse A nicht demjenigen Bereiche angehört, dessen Grössen wir als rational ansehen.

Die Wurzeln dieser Gleichung sind, falls x_1 eine derselben bedeutet,

$$x_1, \quad \omega x_1, \quad \omega^2 x_1, \ \ldots \ \omega^{p-1} x_1 \quad (\omega^p = 1).$$

Dann ist der Quotient zweier Wurzeln gleich einer Potenz der primitiven p^{ten} Einheitswurzel ω. Eine passend gewählte Potenz dieses Quotienten ist gleich ω selbst. Es ist also, wenn zwei Wurzeln x_β, x_γ gegeben sind, jede dritte durch

$$x_\alpha = x_\beta \left(\frac{x_\beta}{x_\gamma}\right)^m = \frac{{x_\beta}^{m+1}}{{x_\gamma}^m},$$

d. h. rational durch x_β und x_γ darstellbar.

Sobald sich demnach die Irreduktibilität der Gleichung

$$x^p - A = 0$$

nachweisen lässt, ist dargelegt, dass sie zum Geschlechte der Galois'schen Gleichungen gehört.

Wäre das Gleichungspolynom zerlegbar

$$x^p - A = \varphi_1(x) . \varphi_2(x) \ldots,$$

so könnten, da p eine Primzahl ist, die sämtlichen einzelnen Faktoren nur dann von gleichem Grade sein, wenn dieser Grad gleich 1 wird; dann wären aber alle Wurzeln rational. Diese Möglichkeit ist also zu verwerfen.

Es sei daher $\varphi_1(x)$ von höherem Grade als $\varphi_2(x)$. Die Wurzeln von

$$\begin{aligned} \varphi_1(x) &\quad \text{seien} \quad x'_1, x'_2, x'_3, \ldots, x'_{n_1}, \\ \varphi_2(x) &\quad \text{„} \quad x''_1, x''_2, x''_3, \ldots, x''_{n_2}. \end{aligned}$$

Dann wird der letzte Koefficient in jedem der Polynome φ_1, φ_2 respektive

$$\begin{aligned} \pm x'_1 x'_2 x'_3 \ldots &= \pm \omega^{\sigma_1} x_1^{n_1}, \\ \pm x''_1 x''_2 x''_3 \ldots &= \pm \omega^{\sigma_2} x_1^{n_2} \end{aligned} \qquad n_1 > n_2$$

im Rationalitätsgebiete rational sein, also auch ihr Quotient

$$\pm \omega^{\tau} x_1^{m}, \quad m > 0.$$

Da p eine Primzahl ist, so ist es möglich, eine ganze Zahl μ so zu bestimmen, dass die Kongruenz

$$m\mu \equiv 1 \pmod{p}$$

oder die Gleichung

$$m\mu = \nu p + 1$$

befriedigt wird. Daher wird

$$(\pm x_1^{m} \omega^{\tau})^{\mu} = \pm x_1^{\nu p + 1} \omega^{\mu\tau} = \pm A^{\nu} x_1 \omega^{\mu\tau} = \pm A^{\nu} x'$$

rational und also x' selbst. Aus der Zerlegbarkeit unserer Gleichung würde somit die Rationalität einer Wurzel folgen. Diese ist aber sicher nicht vorhanden.

Die Gruppe der Gleichung ist von der Ordnung $p(p-1)$. Denn lässt man eine Wurzel x_1 ungeändert, so kann eine andere $x_1\omega$ in jede der übrigen $x_1\omega$, $x_1\omega^2$, $x_1\omega^3$, $\ldots$ $x_1\omega^{p-1}$, also in $p-1$ Wurzeln übergeführt werden. Hier ist somit die Zahl σ des vorigen Paragraphen gleich 1 zu setzen.

Lehrsatz IV. Die binomische Gleichung

$$x^p - A = 0,$$

bei welcher A nicht die vollkommene Potenz einer dem Rationalitätsbereiche angehörigen Grösse ist, gehört zu den Galois'schen Gleichungen. Ihre Gruppe hat die Ordnung $p(p-1)$.

§ 191. Anmerkung. Es fehlen uns fürs erste noch die Mittel, um den dritten Lehrsatz umzukehren. Es kann daher erst im nächsten Kapitel mit algebraischen Hilfsmitteln und wird dann später noch einmal bei der gruppen-theoretischen Behandlung auflösbarer Gleichungen gezeigt werden, dass jede Gleichung eines Primzahlgrades, welche irreduktibel und auflösbar ist, eine Galois'sche oder eine Abel'sche Gleichung sein muss. Bevor wir aber zu solchen allgemeinen Betrachtungen übergehen, wollen wir noch einen Spezialfall betrachten, bei dem rationale Beziehungen zwischen drei und drei Wurzeln einer Gleichung bestehen.

---

§ 192. Wir sagen von einer Gleichung, sie besitze Tripelcharakter, oder wir nennen sie auch kurz eine Tripelgleichung*, wenn ihre Wurzeln zu Tripeln x_α, x_β, x_γ derart angeordnet werden können, dass zwei Elemente eines Tripels durch eine rationale Beziehung eindeutig das dritte Element bestimmen, also x_α und x_β das Element x_γ, ebenso x_α und x_γ das Element x_β und endlich x_β und x_γ das Element x_α.

Die Gleichungen dritten Grades sind Tripelgleichungen, da

ist. $$x_1 + x_2 + x_3 = c_1$$

Von Gleichungen höherer Grade können ferner Gleichungen siebenten Grades Tripelcharakter besitzen. Hier ist z. B. folgende Anordnung der sieben Wurzeln $x_1, x_2, \ldots x_7$ möglich:

$$x_1, x_2, x_3; \quad x_1, x_4, x_5; \quad x_1, x_6, x_7; \quad x_2, x_4, x_6; \quad x_2, x_5, x_7; \quad x_3, x_4, x_7.$$

Ist n der Grad der Gleichung, so kann man $\frac{n(n-1)}{2}$ Kombinationen x_α, x_β von je zwei Wurzeln bilden. Zu jeder von diesen gehört eine dritte Wurzel x_γ, also ein Tripel. Jedes dieser Tripel kommt dreimal vor, jenachdem man als anfängliche Kombination zweier Wurzeln x_α, x_β; x_α, x_γ; x_β, x_γ nimmt. Es giebt also $\frac{n(n-1)}{6}$ Tripel. Da dieser Bruch eine ganze Zahl bedeuten muss, so wird nur für $n = 6m+1$, $n = 6m+3$ ein Tripelcharakter existieren können. $n = 6m$ ist auszuschliessen, da n ungerade sein muss, wie man erkennt, wenn man x_1 mit allen übrigen Elementen kombiniert, die sich demnach zu je zwei und zwei anordnen.

Es bleibe dahingestellt, ob es für jedes $n = 6m+1$, $n = 6m+3$ Tripelsysteme giebt.

---

* Noether: Math. Ann. XV, p. 89.

Da man leicht ein Verfahren aufstellen kann, aus einem Tripelsysteme von n Elementen ein solches von $2n+1$ Elementen abzuleiten, und aus zwei Tripelsystemen der Grade n_1, n_2 ein solches vom Grade $n_1 . n_2$, so folgt aus der Existenz des Systems für $n=3$ z. B. die für $n=7, 15, 31, \ldots$; $9, 19, 39, \ldots$; $21, 43, \ldots$; hierdurch sind aber nicht alle Systeme erschöpft; so existieren Systeme für $n=13$ u. s. f.

§ 193. Wir wollen ein Verfahren auseinandersetzen, aus zwei Tripelsystemen der Grade n_1, n_2 ein drittes vom Grade $n_1 . n_2$ zu bilden. Die Indices des ersten Systemes mögen durch $a, b, c, \ldots$, die des zweiten durch $\alpha, \beta, \gamma, \ldots$ bezeichnet werden.

Die Tripel deuten wir durch die Angabe der entsprechenden Elementen-Indices an. So mag das erste System die Tripel besitzen

T_1) $\qquad a, b, c; \quad a, d, e; \quad b, d, g; \ldots$

ferner seien die des zweiten charakterisiert durch

T_2) $\qquad \alpha, \beta, \gamma; \quad \alpha, \delta, \varepsilon; \quad \alpha, \zeta, \eta; \ldots$

Die Elemente des kombinierten Systems seien $x_{a\alpha}$, $x_{a\beta}$, $x_{b\alpha}$, $\ldots$ Wir bilden folgendermassen ein Tripelsystem für dieselben. Zuerst schieben wir hinter jedes Element von T_1) das Element α; dadurch entstehen $\frac{n_1(n_1-1)}{6}$ Tripel der Elemente mit doppelten Indices.

Ferner schieben wir β, dann γ, darauf $\delta, \ldots$ und so jeden der n_2 Indices des zweiten Systems hinter jeden Index jedes Tripels T_1). Dadurch entstehen jedesmal $\frac{n_1(n_1-1)}{6}$ und im ganzen

$$n_2 \frac{n_1(n_1-1)}{6}$$

Tripel unter den Elementen $x_{a\alpha}$, $x_{a\beta}$, $x_{a\gamma}$, $\ldots$ $x_{b\alpha}$, $x_{b\beta}$, $\ldots$ Alle diese sind von einander verschieden; es sind:

T'_3)
$$\left\{\begin{array}{llll} a\alpha, b\alpha, c\alpha; & a\alpha, d\alpha, e\alpha; & b\alpha, d\alpha, g\alpha; & \ldots \\ a\beta, b\beta, c\beta; & a\beta, d\beta, e\beta; & b\beta, d\beta, g\beta; & \ldots \\ a\gamma, b\gamma, c\gamma; & a\gamma, d\gamma, e\gamma; & b\gamma, d\gamma, g\gamma; & \ldots \\ \ldots & \ldots & \ldots & \end{array}\right.$$

Ferner schieben wir jeden Index des ersten Systems vor jeden in T_2) auftretenden Index; dadurch erhalten wir

$$n_1 \frac{n_2(n_2-1)}{6}$$

Tripel unter denselben $n_1 . n_2$ Elementen, die durch je zwei Indices bestimmt sind. Auch diese sind unter sich und von denen aus T'_3) verschieden; sie sind in folgender Tabelle enthalten:

$$T''_3) \quad \left| \begin{array}{lll} a\alpha,\ a\beta,\ a\gamma; & a\alpha,\ a\delta,\ a\varepsilon; & a\alpha,\ a\xi,\ a\eta;\ \ldots \\ b\alpha,\ b\beta,\ b\gamma; & b\alpha,\ b\delta,\ b\varepsilon; & b\alpha,\ b\xi,\ b\eta;\ \ldots \\ c\alpha,\ c\beta,\ c\gamma; & c\alpha,\ c\delta,\ c\varepsilon; & c\alpha,\ c\xi,\ c\eta;\ \ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & \end{array} \right.$$

Endlich kombinieren wir je ein Tripel von T_1) mit einem Tripel von T_2) derart, dass hinter jedes der drei Elemente eines Tripels aus T_1) je ein Element eines Tripels aus T_2) tritt. Es kann dies, falls die beiden Tripel einmal festgelegt sind, auf sechs wesentlich von einander verschiedene Arten geschehen, z. B. mit b, d, e und α, ξ, η so:

$$b\alpha,\ d\xi,\ g\eta;\quad b\alpha,\ d\eta,\ g\xi;\quad b\xi,\ d\alpha,\ g\eta;\quad b\xi,\ d\eta,\ g\alpha;\quad b\eta,\ d\alpha,\ g\xi;$$
$$b\eta,\ d\xi,\ g\alpha.$$

Man erhält demnach aus T_1), T_2) als Zahl solcher Kombinationen

$$6\,\frac{n_1(n_1-1)}{6}\cdot\frac{n_2(n_2-1)}{6}=n_1n_2\,\frac{n_1n_2-n_1-n_2+1}{6}.$$

Auch sie sind unter sich und von denjenigen, welche in T'_3) und T''_3) vorkommen, verschieden.

Alle diese nehmen wir in folgende Tabelle auf:

$$T'''_3) \quad \left| \begin{array}{llll} a\alpha,\ b\beta,\ c\gamma; & a\alpha,\ b\gamma,\ c\beta; & a\beta,\ b\alpha,\ c\gamma; & \ldots\ a\gamma,\ b\beta,\ c\alpha; \\ a\alpha,\ b\delta,\ c\varepsilon; & a\alpha,\ b\varepsilon,\ c\delta; & a\delta,\ b\alpha,\ c\varepsilon; & \ldots\ a\varepsilon,\ b\delta,\ c\alpha; \\ a\alpha,\ d\beta,\ e\gamma; & a\alpha,\ d\gamma,\ e\beta; & a\beta,\ d\alpha,\ e\gamma; & \ldots\ a\gamma,\ d\beta,\ e\alpha; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & \end{array} \right.$$

Wir haben demnach jetzt zwischen den $n_1 . n_2$ Elementen

$$x_{a\alpha},\ x_{a\beta},\ x_{a\gamma},\ \ldots;\ x_{b\alpha},\ x_{b\beta},\ x_{b\gamma},\ \ldots;\ \ldots$$

aufgestellt eine Anzahl von

$$n_2\,\frac{n_1(n_1-1)}{6}+n_1\,\frac{n_2(n_2-1)}{6}+n_1n_2\,\frac{n_1n_2-n_1-n_2+1}{6}=\frac{n_1n_2(n_1n_2-1)}{6}$$

von einander verschiedener Tripel. Folglich bilden die drei Tabellen T_3) eins der für $n_1 . n_2$ Elemente möglichen Tripelsysteme.

§ 194. Um die zu einer Tripelgleichung gehörige Gruppe G zu finden, braucht man nur zu bedenken, dass die Substitutionen derselben den Tripelcharakter der Gleichung nicht zerstören dürfen; die Gruppe G enthält also alle und nur diejenigen Substitutionen, welche das Tripelsystem in sich selbst umwandeln. Ist etwa T_1) aus § 193 das Tripelsystem der Gleichung, und versteht man unter dem Symbol

$$(p,\ q,\ r)$$

eine allgemeine symmetrische Funktion der drei Elemente x_p, x_q, x_r, so wird

$$\varphi = (a, b, c) + (a, d, e) + (b, d, g) + \ldots$$

eine zur Gattung der Gruppe gehörige Funktion sein. Die Gruppe G enthält alle Substitutionen, welche φ nicht ändern. φ ist daher rational bekannt; es ist die Gattung von φ der Gleichung mit Tripelcharakter adjungiert.

Von dieser Gruppe sind einige allgemeine Eigenschaften ersichtlich:

1) Jede Substitution der Gruppe, welche zwei beliebige Elemente ungeändert lässt, lässt auch ein drittes ungeändert; dasjenige nämlich, welches mit jenen beiden zu demselben Tripel gehört. Ein solches Element wollen wir das jenen beiden conjugierte nennen.

Daher kann die Gruppe einer Tripelgleichung höchstens zweifach transitiv sein; denn sobald der Ort für zwei Elemente bestimmt ist, darf ihr konjugiertes Element nicht willkürlich umgesetzt werden.

2) Lässt eine Substitution m Elemente ungeändert, so lässt sie noch α andere ungeändert, wo $m + \alpha$ von der Form $6k + 1$, $6k + 3$ sein muss. α kann natürlich auch $= 0$ sein. Denn diejenigen Tripel, welche zwei der m Elemente enthalten, enthalten auch ein drittes; die festen Elemente bilden somit ein Tripelsystem.

3) Kommen in der Gruppe Substitutionen s', s'', ... vor, welche genau m Elemente

$$x_1, x_2, x_3, \ldots x_m$$

ungeändert lassen, und andere Substitutionen t', t'', ..., welche ausser diesen Elementen noch andere, also z. B.

$$x_1, x_2, \ldots x_m, x_{m+1}, \ldots x_{m+\alpha}$$

ungeändert lassen, so ist α mindestens gleich $m + 1$. Denn t' kann keinen der Tripel ändern, welche zu den Kombinationen zweiter Klasse

$$x_1 x_{m+1}, x_2 x_{m+1}, x_3 x_{m+1}, \ldots x_m x_{m+1}$$

gehören. Die zu diesen Kombinationen gehörigen konjugierten Elemente sind sämtlich von einander verschieden; also lässt t' mindestens $2m + 1$ Elemente ungeändert.

4) Bedeuten x_a, x_b, x_c die drei Elemente eines Tripels, so lässt jede Substitution, welche die Folge $x_a x_b x_c$ enthält, auf x_c wieder x_a folgen, d. h. sie enthält den Cyklus $(x_a x_b x_c)$.

Lässt eine Substitution das Element x_a ungeändert, während sie auf x_b folgen lässt x_c, so muss sie auf x_c wiederum x_b folgen lassen, d. h. sie enthält die Transposition $(x_b x_c)$.

5) Die zu dem Tripelsystem T_3) aus § 193 gehörige Gruppe enthält eine Untergruppe, welche nur die zweiten Indices, und eine andere,

welche nur die ersten Indices vertauscht. Jene lässt den Komplex T'_3), diese den Komplex T''_3) ungeändert.

6) Da die Tripelgleichung eine $\frac{n(n-1)}{6}$-wertige Resolvente hat, nämlich diejenige, welche oben mit

$$(p, q, r)$$

bezeichnet wurde, so werden alle ihre Werte durch die Auflösung einer Gleichung vom Grade $\frac{n(n-1)}{6}$ gefunden. Die Ordnung der Gruppe dieser Gleichung ist also

$$\frac{1}{\sigma}\left(\frac{n(n-1)}{6}!\right).$$

Ist (p, q, r) bekannt, so folgen x_p, x_q, x_r daraus durch eine Gleichung $(x-x_p)(x-x_q)(x-x_r)=0$, welche die Substitutionen

$$1, (x_p x_q x_r), (x_p x_r x_q), (x_p x_q), (x_p x_r), (x_q x_r)$$

zur Gruppe hat. Alle Wurzeln werden nach der Lösung dieser durch quadratische Gleichungen bestimmt. Denn wenn x_p bekannt ist, so wird die Gleichung

$$(x-x'_p)(x-x'_q)(x-x'_r)=0$$

nach Adjungierung der Wurzel x_p zerfallen. Solcher Gleichungen giebt es noch $(n-3):2$. Die Tripelgleichung hat also eine Gruppe, deren Ordnung ein Teiler wird von

$$6(n-3)\cdot\left(\frac{n(n-1)}{6}!\right).$$

§ 195. Wir legen jetzt bei den Bildungen von § 193 die beiden Tripelsysteme T_1) und T_2) von je drei Elementen, von denen auch nur die Indices angegeben werden sollen

T_1) (0, 1, 2) und T_2) (0, 1, 2)

zu Grunde. Aus ihrer Kombination entsteht

T'_3) (00, 10, 20), (01, 11, 21), (02, 12, 22),

T''_3) (00, 01, 02), (10, 11, 12), (20, 21, 22),

T'''_3) (00, 11, 22), (00, 12, 21), (01, 10, 22),
(01, 12, 20), (02, 10, 21), (02, 11, 20).

Behalten wir die doppelten Indices bei und kombinieren wir diese neue Gruppe T_3) wiederum mit T_2), so entsteht ein Tripelsystem von 27 Elementen, welche durch je drei Indices charakterisiert sind

000, 001, 002, 010, 011, 012, ... 220, 221, 222.

Bezeichnen wir ein solches Element durch pqr, so ist es leicht, die Bedingung dafür aufzustellen, dass

T_4) $\qquad (pqr,\ p'q'r',\ p''q''r'')$

ein Tripel wird. Denn für $p, q;\ p', q';\ p'', q''$ gelten, wie man sieht, die Beziehungen

$$p+p'+p''\equiv q+q'+q''\equiv 0 \pmod 3,$$

damit die Kombination

$$(pq,\ p'q',\ p''q'')$$

ein Tripel in dem Systeme der 9 Elemente werde. Nach § 193 ist nun in T) entweder $(rr'r'')=(012)$ oder $r=r'=r''$. Ferner ist nach § 193 $(pq,\ p'q',\ p''q'')$ entweder ein Tripel in T_3) oder $p=p'=p''$, $q=q'=q''$; also wird auch bei T_4) die notwendige und hinreichende Bedingung für die Tripeleigenschaft die sein, dass die Kongruenzen stattfinden

B) $\qquad p+p'+p''\equiv q+q'+q'''\equiv r+r'+r'''\equiv 0 \pmod 3.$

Offenbar kann man in genau derselben Weise zu 3.27 Elementen übergehen. Wir bleiben hier stehen, weil die allgemeinen Entwickelungen für $n=3^x$ dieselben sind, die Schreibweise aber unübersichtlich wird.

Die zu dem Tripelsystem T_4) von 27 Elementen gehörige Gruppe enthält alle und nur diejenigen Substitutionen, welche die Gesamtheit der Tripel in sich selbst umwandelt. Dahin gehören sicher die Substitutionen von der Form

$$s=|p,\ q,\ r \quad ap+bq+cr+\alpha,\ a'p+b'q+c'r+\alpha',\ a''p+b''q+c''r+\alpha''|.$$

Dieses Symbol sagt aus, dass die Indices p, q, r respektive durch

$$ap+bq+cr+\alpha,\ a'p+b'q+c'r+\alpha',\ a''p+b''q+c''r+\alpha''$$

ersetzt werden sollen (vergl. § 136). Führt man nun diese Ausdrücke in B) ein, so werden auch die neuen Kongruenzen, als lineare Kombinationen der alten, erfüllt sein.

Umgekehrt kann jede Substitution, die das Tripelsystem ungeändert lässt, durch geeignete Wahl der $a, b, c, \alpha;\ a', b', \ldots$ in der Form von s erhalten werden. Denn ist t_1 eine der Tripelgruppe zugehörige Substitution, welche das Element (000) in $(\alpha\alpha'\alpha'')$ umwandelt, und ist

$$s_1=|p,\ q,\ r \quad p+\alpha,\ q+\alpha',\ r+\alpha''|,$$

so wird $t_2=t_1^{+1}s_1^{-1}$ zur Gruppe gehören und (000) ungeändert lassen.

Wenn t_2 nun (001) in $(cc'c'')$ umwandelt, wo die drei c nicht sämtlich Null sein können, da (000) ungeändert bleibt, und man setzt mit willkürlichen $a, a', a'';\ b, b', b''$

$$s_2 = |p,\ q,\ r \quad ap+bq+cr,\ a'p+b'q+c'r,\ a''p+b''q+c''r|,$$

so wird s_2 auf (000) und (001) folgen lassen (000) respektive $(cc'c'')$. Daher wird $t_3 = t_2^{+1} s_2^{-1}$ die beiden Elemente (000) und (001) ungeändert lassen.

Wenn t_3 ferner (010) in $(dd'd'')$ umändert, so wählen wir mit willkürlichen e, e', e'' die Substitution

$$s_3 = |p,\ q,\ r \quad ep+dq,\ e'p+d'q,\ e''p+d''q+r|,$$

welche (000) und (001) ungeändert und auf (010) folgen lässt $(dd'd'')$. Daher wird $t_4 = t_3^{+1} s_3^{-1}$ die Elemente (000), (001), (010) ungeändert lassen.

Wenn endlich t_4 auf (100) folgen lässt $(gg'g'')$, so bilden wir

$$s_4 = |p,\ q,\ r \quad gp,\ g'p+q,\ g''p+r|;$$

dann lässt s_4 die Elemente (000), (001), (010) ungeändert, während auf (100) folgt $(gg'g'')$.

Daher wird $t_5 = t_4^{+1} s_4^{-1} = t_1 . (s_1^{-1} s_2^{-1} s_3^{-1} s_4^{-1})$ die vier Elemente

$$(000),\ (001),\ (010),\ (100)$$

nicht ändern, dabei aber zur Gruppe des Tripelsystems gehören.

Wir behaupten jetzt, dass man $t_5 = 1$ und infolgedessen setzen könne

$$t_1 = s_4 s_3 s_2 s_1.$$

Es wird nämlich, da t_5 die beiden Elemente (000), (001) nicht umstellt, auch ihr konjugiertes Element (002) an seinem Platze bleiben. Da t_5 ausserdem (010) nicht verändert, so lässt es nach § 194, 3) mindestens 7 Elemente unberührt. Diese haben, wie (000), (001), (010) die Form $(0qr)$. Es giebt jedoch nur 9 derartige Elemente und ausserdem existiert eine Substitution, welche alle diese ungeändert lässt und gleichwohl der Tripelgruppe angehört, nämlich

$$\tau = |p,\ q,\ r \quad 2p,\ q,\ r|.$$

Liesse t_5 nun 7 oder 8 Elemente und nicht jene 9 sämtlich ungeändert, so müsste es nach § 194, 3) mindestens $2.7+1$ oder $2.8+1$ Elemente $(0qr)$ ungeändert lassen. Das ist nicht möglich; demnach lässt t_5 alle 9 Elemente der Form $(0qr)$ unberührt. Endlich versetzt t_5 auch (100) nicht; folglich lässt es mindestens $2.9+1$ Elemente ungeändert. Blieben mehr als 2.9 aber weniger als 3.9 an ihren Plätzen, z. B. $2.9+\alpha$ $(\alpha > 1, < 9)$, so träte, da es eine Substitution $\tau = 1$ giebt, welche alle 3.9 Elemente ungeändert lässt, derselbe Widerspruch gegen § 194, 3) auf, wie oben. Also ist $t_5 = 1$.

Es bilden demgemäss alle und nur die Substitutionen von der Form

$$s \equiv | p,\ q,\ r \quad ap+bq+cr+\alpha,\ a'p+b'q+c'r+\alpha',\ a''p+b''q+c''r+\alpha'' | \pmod 3$$

die Gruppe G des Tripelsystems. Damit dieses Symbol eine Substitution darstelle, ist es nach § 140 notwendig und hinreichend, dass die Determinante

$$\begin{vmatrix} a, & b, & c \\ a', & b', & c' \\ a'', & b'', & c'' \end{vmatrix} \pmod 3$$

von Null verschieden sei; und nach § 142 giebt es $3^3(3^3-1)(3^3-3)(3^3-3^2)$ Substitutionen. Diese Zahl giebt deswegen die Ordnung der Tripelgruppe der 27 Elemente an.

§ 196. Um die allgemeinen Verhältnisse übersehen zu können, ohne durch unübersichtliche Schreibweise gestört zu werden, nehmen wir $n = 3^4$ und setzen

$$s \equiv$$
$$| z_1, z_2, z_3, z_4 \quad a_1z_1+b_1z_2+c_1z_3+d_1z_4+\alpha_1, \ldots, a_4z_1+b_4z_2+c_4z_3+d_4z_4+\alpha_4 | \pmod 3.$$

Ist die Bedingung, dass

$$\begin{vmatrix} a_1, & b_1, & c_1, & d_1 \\ a_2, & b_2, & c_2, & d_2 \\ a_3, & b_3, & c_3, & d_3 \\ a_4, & b_4, & c_4, & d_4 \end{vmatrix} \pmod 3$$

nicht kongruent Null sei, gewahrt, so stellen die Substitutionen der Form s alle und nur die Substitutionen der hier betrachteten Tripelgruppe G von 3^4 Elementen dar. Es giebt

$$r = 3^4(3^4-1)(3^4-3^1)(3^4-3^2)(3^4-3^3)$$

solcher Substitutionen; r ist die Ordnung der Gruppe G.

Wir heben aus ihr diejenige Untergruppe H heraus, für welche

$$a_4 \equiv b_4 \equiv c_4 \equiv 0, \quad d_4 \equiv d$$

ist. Dann darf d zwei Werte 1, 2 annehmen; d_1, d_2, d_3 und $\alpha_1, \ldots \alpha_4$ je drei; die übrigen Elemente müssen die Bedingung, dass

$$\begin{vmatrix} a_1, & b_1, & c_1 \\ a_2, & b_2, & c_2 \\ a_3, & b_3, & c_3 \end{vmatrix} \pmod 3$$

inkongruent Null sei, erfüllen. Die Anzahl der Substitutionen dieser Untergruppe H ist somit $2 \cdot 3^7 (3^3-1)(3^3-3)(3^3-3^2)$.

Ist φ_1 eine zu dieser Gruppe H gehörige Funktion, so ist die Anzahl ihrer Werte nach § 43 gleich dem Quotienten aus der Ordnung der Tripelgruppe G und derjenigen der Untergruppe H, d. h. also gleich

$$\frac{3^4(3^4-1)(3^4-3)(3^4-3^2)(3^4-3^3)}{2 \cdot 3^7 (3^3-1)(3^3-3)(3^3-3^2)} = \frac{3^4-1}{2}.$$

Wir werden im vierzehnten Kapitel sehen, dass die Auffindung dieser Werte von der Lösung einer Gleichung abhängt, deren Gruppe H_1 die allgemeinste ausgezeichnete, in H enthaltene Untergruppe von G ist. Diese suchen wir auf.

Die Form der Substitutionen von H_1 ist

$$t_1 \equiv |z_1, z_2, z_3, z_4 \quad a_1 z_1 + b_1 z_2 + c_1 z_3 + d_1 z_4 + \alpha_1, \ldots \\ a_3 z_1 + b_3 z_2 + c_3 z_3 + d_3 z_4 + \alpha_3, \; d z_4 + \alpha_4 | \pmod 3;$$

ihre charakteristische Eigenschaft, dass die Transformierte von t_1 durch eine beliebige Substitution von G dieselbe Form wie t_1 besitzt.

Wir wählen für die Transformation von t_1

$$u = |z_1, z_2, z_3, z_4 \quad z_1, z_2, z_3, z_4 - z_1|,$$

die Substitution u^{-1} wird dabei

$$u^{-1} = |z_1, z_2, z_3, z_4 \quad z_1, z_2, z_3, z_4 + z_1|$$

und das Produkt $u^{-1} t u$ führt z_4 in

$$(a_1 - d_1 - d) z_1 + b_1 z_2 + c_1 z_3 + (d + d_1) z_4 + \alpha_1 + \alpha_4$$

über. Da dies die Form $d' z_4 + \alpha'$ haben muss, so folgt

$$a_1 \equiv d + d_1, \quad b_1 \equiv 0, \quad c_1 \equiv 0.$$

Ebenso findet man durch entsprechende Transformationen

$$a_2 \equiv 0, \quad b_2 \equiv d + d_2, \quad c_2 \equiv 0, \\ a_3 \equiv 0, \quad b_3 \equiv 0, \quad c_3 \equiv d + d_3,$$

so dass die Form der Substitutionen von H_1 nur sein kann

$$t_2 = |z_1, z_2, z_3, z_4 \quad (d+d_1) z_1 + d_1 z_4 + \alpha_1, \ldots, (d+d_3) z_3 + d_3 z_4 + \alpha_3, \; d z_4 + \alpha_4|.$$

Transformieren wir jetzt durch v, wo

$$v = |z_1, z_2, z_3, z_4 \quad z_1, z_2, z_3, z_4 - z_1 - z_2|, \\ v^{-1} = |z_1, z_2, z_3, z_4 \quad z_1, z_2, z_3, z_4 + z_1 + z_2|,$$

so findet sich $d_1 = 0$, $d_2 = 0$; ähnliche Transformationen liefern $d_3 = 0$, so dass die Form der Substitutionen von H_1 sich reduziert auf

$$t_3 \equiv |z_1, z_2, z_3, z_4 \quad d z_1 + \alpha_1, \; d z_2 + \alpha_2, \; d z_3 + \alpha_3, \; d z_4 + \alpha_4| \pmod 3.$$

Um zu zeigen, dass diese letzte Form auch hinreichend ist, transformieren wir t_3 durch w, wobei

$$w^{-1} = |z_1, z_2, z_3, z_4 \quad a'z_1 + b'z_2 + c'z_3 + d'z_4 + \alpha', \ldots, \; a^{(4)}z_1 + b^{(4)}z_2 + \ldots + \alpha^{(4)}|.$$

Danach wird die inverse Substitution w selbst lauten:

$$w = \Big| z_1, z_2, z_3, z_4 \quad \frac{1}{\Delta}\left(\frac{\partial \Delta}{\partial a'}(z_1 - \alpha') + \frac{\partial \Delta}{\partial a''}(z_2 - \alpha'') + \ldots\right),$$
$$\frac{1}{\Delta}\left(\frac{\partial \Delta}{\partial b'}(z_1 - \alpha') + \frac{\partial \Delta}{\partial b''}(z - \alpha'') + \ldots\right), \ldots \Big|.$$

Wendet man nun w^{+1} transformierend auf t_3 an und bildet also $w^{-1}t_3w$, so geht z. B. z_4 der Reihe nach über in $a^{(4)}z_1 + b^{(4)}z_2 + \ldots + \alpha^{(4)}$, dann in $a^{(4)}(dz_1 + \alpha_1) + b^{(4)}(dz_1 + \alpha_2) + \ldots$, endlich in

$$a^{(4)}d\left[\frac{1}{\Delta}\frac{\partial \Delta}{\partial a'}z_1 + \ldots\right] + b^{(4)}d\left[\frac{1}{\Delta}\frac{\partial \Delta}{\partial b'}z_1 + \ldots\right] + \ldots$$

Ordnet man nach z_1, z_2, z_3, ..., so werden wegen der Determinanteneigenschaften die Koefficienten von z_1, z_2, z_3, d. h.

$$\frac{d}{\Delta}\left(a^{(4)}\frac{\partial \Delta}{\partial a'} + b^{(4)}\frac{\partial \Delta}{\partial b'} + \ldots\right), \quad \frac{d}{\Delta}\left(a^{(4)}\frac{\partial \Delta}{\partial a''} + b^{(4)}\frac{\partial \Delta}{\partial b''} + \ldots\right),$$
$$\frac{d}{\Delta}\left(a^{(4)}\frac{\partial \Delta}{\partial a'''} + b^{(4)}\frac{\partial \Delta}{\partial b'''} + \ldots\right)$$

verschwinden, während der Koefficient von z_4 gleich d wird. Das Gleiche gilt von z_1, z_2, z_3. H_1 enthält also die $2 \cdot 3^4$ Substitutionen der Form t_3.

Die Untersuchungen des vierzehnten Kapitels führen, wie schon erwähnt, zu den Resultaten: Alle Werte von φ_1 hängen von einer Gleichung des Grades $\frac{3^4 - 1}{2}$ ab, deren Gruppe die Ordnung

$$r' = \frac{r}{r_1} = \frac{3^4(3^4 - 1)(3^4 - 3)(3^4 - 3^2)(3^4 - 3^3)}{2 \cdot 3^4} = 3^6 \cdot 80 \cdot 26 \cdot 8$$

besitzt. Ist dieselbe gelöst, so reduziert sich die Gruppe der Tripelgleichung auf die Gruppe H_1, welche aus den Substitutionen der Form

$$t_3 = |z_1, z_2, z_3, z_4 \quad dz_1 + \alpha_1, \; dz_2 + \alpha_2, \; dz_3 + \alpha_3, \; dz_4 + \alpha_4| \pmod 3$$

gebildet ist. Ihre Ordnung r_1 ist gleich $2 \cdot 3^4$.

Aus H_1 bilden wir behufs weiterer Reduktion eine Untergruppe J, welche alle Substitutionen der Form t_3 enthält, bei denen $\alpha_4 = 0$ ist. Es sei φ_2 eine zu J gehörige Substitution. Ist φ_2 bekannt, so reduziert sich die Gruppe H_1 auf die allgemeinste ausgezeichnete Unter-

gruppe von H_1, welche in J enthalten ist. Diese Gruppe heisse H_2; wir wollen dieselbe zu bestimmen suchen.

Die Substitutionen τ dieser Gruppe müssen die Form haben

$$\tau_1 = |z_1, z_2, z_3, z_4 \quad d'z_1 + \alpha'_1,\ d'z_2 + \alpha'_2,\ d'z_3 + \alpha'_3,\ d'z_4|.$$

Nehmen wir t_3 in der obigen Form, so wird

$$t_3^{-1} = \left| z_1, z_2, z_3, z_4 \quad \frac{1}{d}(z_1 - \alpha_1),\ \frac{1}{d}(z_2 - \alpha_2),\ \frac{1}{d}(z_3 - \alpha_3),\ \frac{1}{d}(z_4 - \alpha_4) \right|$$

und $t_3 \tau t_3^{-1}$ setzt z_4 nacheinander in

$$dz_4 + \alpha_4, \quad dd'z_4 + \alpha_4, \quad d'(z_4 - \alpha_4) + \alpha_4$$

um; damit das letztere keine Konstante habe, muss $d' = 1$ sein. Dies ist auch ausreichend, und daher besteht H_2 aus allen Substitutionen der Form $\tau_2 = |z_1, z_2, z_3, z_4 \quad z_1 + \alpha_1,\ z_2 + \alpha_2,\ z_3 + \alpha_3,\ z_4|$ und ist von der Ordnung 3^3.

φ_2 kann aus φ_1 durch Auflösung einer Gleichung abgeleitet werden, deren Ordnung

$$r'' = \frac{r_1}{r_2} = \frac{2 \cdot 3^4}{3^3} = 2 \cdot 3$$

ist. Dadurch reduziert sich die Gruppe H_1 von φ_1 auf die Gruppe H_2, welche aus den Substitutionen von der Form

$$\tau_2 = |z_1, z_2, z_3, z_4 \quad z_1 + \alpha_1,\ z_2 + \alpha_2,\ z_3 + \alpha_3,\ z_4|$$

besteht. Ihre Ordnung r_2 ist gleich 3^3.

In gleicher Weise kann man aus H_2 eine Untergruppe K durch diejenigen Substitutionen bilden, in denen α_3 gleich Null ist. Es sei φ_3 eine zu K gehörige Funktion. Ist φ_3 bekannt, so reduziert sich die Gruppe H_2 auf die allgemeinste ausgezeichnete Untergruppe H_3 von H_2, welche in K enthalten ist. Man erkennt ohne Schwierigkeit, dass

$$H_2^{-1} K H_2 = K,$$

dass also $H_3 = K$ ist. Dann nimmt man weiter eine Untergruppe L von H_3, in der $\alpha_2 = 0$ ist u. s. w. Demnach ergiebt sich:

Bestimmt man der Reihe nach zu den Gruppen

H_3, bestehend aus $\tau_3 = |z_1, z_2, z_3, z_4 \quad z_1 + \alpha_1,\ z_2 + \alpha_2,\ z_3,\ z_4|$,

H_4, „ „ $\tau_4 = |z_1, z_2, z_3, z_4 \quad z_1 + \alpha_1,\ z_2,\ z_3,\ z_4|$

die Funktionen φ_3, φ_4, so kann man von φ_2 zu φ_3 und von φ_3 zu φ_4 durch die Lösung je einer Gleichung gelangen, deren Gruppe die Ordnung 3 besitzt. Von φ_4 endlich kommt man zur vollständigen Lösung der Tripelgleichung wieder durch eine Gleichung, deren Gruppe von der Ordnung 3 ist.

§ 197. Statt von der Gruppe von φ_1 hätten wir mit demselben Erfolge von derjenigen einer anderen Funktion ψ_1 ausgehen können, deren Substitutionen die Form

$$\sigma = | z_1, z_2, z_3, z_4 \quad a_1 z_1 + b_1 z_2 + c_1 z_3 + d_1 z_4 + \alpha_1,\ b_2 z_2 + c_2 z_3 + d_2 z_4 + \alpha_2,$$
$$c_3 z_3 + d_3 z_4 + \alpha_3,\ d_4 z_4 + \alpha_4 |$$

haben. Die Methode des vorigen Paragraphen zeigt, dass die umfassendste ausgezeichnete Untergruppe der Tripelgruppe G, deren Substitutionen von der Form σ sind, mit der Gruppe H_1 des vorigen Paragraphen identisch ist. Eine solche Funktion ψ_1 lässt sich leicht bilden. Es giebt in T_3) drei Tripel, welche zusammen alle neun Elemente enthalten:

A_3) (00, 10, 20), (01, 11, 21), (02, 12, 22).

Schiebt man bei der Bildung von T_4) hinter jedes dieser Tripelelemente 0, 1, 2, so erhält man 9 Tripel, welche zusammen alle 27 Elemente enthalten:

$$A_4)\ \begin{cases} (000, 100, 200), & (010, 110, 210), & (020, 120, 220), \\ (001, 101, 201), & (011, 111, 211), & (021, 121, 221), \\ (002, 102, 202), & (012, 112, 212), & (022, 122, 222). \end{cases}$$

Die gleiche Bildung führt bei $n = 3^4$ auf 27 Tripel A_5), welche zusammen alle 81 Elemente enthalten.

Wir verstehen jetzt, wie oben, unter (p, q, r) eine symmetrische Funktion der eingeschlossenen Elemente; dann lässt sich beweisen, dass jede symmetrische Funktion, welche (bei $n = 3^4$) jene 27 Tripel A_5) zu Elementen hat, zur Gruppe der σ gehört, z. B.:

$$\psi_1 = (0000, 1000, 2000) + \ldots + (0220, 1220, 2220)$$
$$+ (0001, 1001, 2001) + \ldots + (0221, 1221, 2221)$$
$$+ (0002, 1002, 2002) + \ldots + (0222, 1222, 2222).$$

In der That wird jedes σ die Gesamtheit der Tripel einer Zeile, weil sie den gleichen letzten Index haben, in die Gesamtheit der Tripel einer anderen Zeile, bei denen ja dasselbe stattfindet, überführen. Ist durch die Angabe von z_4 und $d_4 z_4 + \alpha_4$ die Reihenfolge dieser Umwandlungen bekannt, so darf für die einzelne Zeile z_4 als konstant angesehen werden, und, statt den aufgestellten Satz zu beweisen, brauchen wir nur zu zeigen, dass die aus A_4) gebildete symmetrische Funktion

$$\chi_3 = (000, 100, 200) + \ldots + (020, 120, 220)$$
$$+ (001, 101, 201) + \ldots + (021, 121, 221)$$
$$+ (002, 102, 202) + \ldots + (022, 122, 222)$$

zu der Gruppe der σ' gehört, welche die Form haben

$$\sigma' = |z_1, z_2, z_3 \quad a_1 z_1 + b_1 z_2 + c_1 z_3 + \alpha'_1,\ b_2 z_2 + c_2 z_3 + \alpha'_2,\ c_3 z_3 + \alpha'_3|$$
$$(\alpha'_1 = \alpha_1 + d_1 z_4, \quad \alpha'_2 = \alpha_2 + d_2 z_4, \quad \alpha'_3 = \alpha_3 + d_3 z_4).$$

Dies ist dieselbe Frage für drei Indices, welche oben für vier zu beweisen war. Dieselbe Reduktion gilt auch hier; so kommt man auf zwei und auf einen Index und dabei ist die Richtigkeit ersichtlich.

Sind alle Werte von ψ_1 bekannt, so reduziert sich die Tripelgruppe auf die durch die Substitutionen t_3 gebildete Gruppe H_1 der Ordnung $2 \cdot 3^4$ (§ 196). Wir bestimmen die Anzahl der Werte von ψ_1. Transformiert man ψ_1 durch irgend eine Substitution von G, so wird das Resultat die Eigenschaft von ψ_1 teilen, alle 3^4 Elemente in 27 Tripeln zu enthalten. Die Gruppe der σ enthält, weil a_1, b_2, c_3, d_4 nur $\equiv 1, 2 \pmod 3$ sein dürfen, während man die übrigen zehn Konstanten willkürlich annehmen kann, $2^4 \cdot 3^{10}$ Substitutionen; da die Ordnung von G gleich

$$3^4(3^4-1)(3^4-3)(3^4-3^2)(3^4-3^3) = 3^{10}(3^4-1)(3^3-1)(3^2-1)(3-1)$$

ist, so hat ψ_1

$$\frac{(3^4-1)(3^3-1)(3^2-1)(3-1)}{2^4} = 40 \cdot 13 \cdot 4$$

Werte, während φ_1 deren nur 40 besass. Es verdient bemerkt zu werden, dass die Gleichungen für ψ_1 und für φ_1, trotzdem die eine vom Grade $40 \cdot 13 \cdot 4$, die andere nur vom Grade 40 ist, durch ihre vollständige Auflösung die Tripelgruppe auf dieselbe ausgezeichnete Untergruppe H_1 reduzieren. Den Grund hiervon haben wir schon oben angedeutet; später werden wir die einschlagenden Verhältnisse genauer betrachten.

Wir gehen von diesen allgemeinen Untersuchungen zu dem Spezialfalle $n = 3^2$, der eine vollständige algebraische Auflösung zulässt, über.

§ 198. Für neun Elemente giebt es nur ein Tripelsystem, wie die wirkliche Bildung sofort zeigt.

Man kann folglich unser bisher behandeltes System für $n = 9$ als das allgemeine ansehen.

Hierbei werden die beiden Funktionen φ_1 und ψ_1 gleichwertig und zwar wird die Anzahl dieser Werte gleich 4. Es hat ψ die Form

$$\psi_1 = (00,\ 10,\ 20) + (01,\ 11,\ 21) + (02,\ 12,\ 22)$$

und die übrigen drei Werte dieser Funktion sind die folgenden:

$$\psi_2 = (00,\ 01,\ 02) + (10,\ 11,\ 12) + (20,\ 21,\ 22),$$
$$\psi_3 = (00,\ 12,\ 21) + (02,\ 11,\ 20) + (01,\ 10,\ 22),$$
$$\psi_4 = (00,\ 11,\ 22) + (01,\ 12,\ 20) + (02,\ 10,\ 21).$$

Diese vier Werte können durch die vollständige Auflösung einer Gleichung des vierten Grades erlangt werden. Wir wollen annehmen, dass diese Lösung bewerkstelligt ist und die Funktionalwerte ψ_1, ψ_2, ψ_3, ψ_4 bekannt sind. Wir haben nun zu setzen

$$\chi_1 = \{z - [00, 10, 20]\}\{z - [01, 11, 21]\}\{z - [02, 12, 22]\},$$
$$\chi_2 = \{z - [00, 01, 02]\}\{z - [10, 11, 12]\}\{z - [20, 21, 22]\},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$[00, 10, 20] = (u - x_{00})(u - x_{10})(u - x_{20}),$$
$$[01, 11, 21] = (u - x_{01})(u - x_{11})(u - x_{21}), \ldots$$
$$[00, 01, 02] = (u - x_{00})(u - x_{01})(u - x_{02}),$$
$$[10, 11, 12] = (u - x_{10})(u - x_{11})(u - x_{12}), \ldots$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

Dann ist χ_1 rational durch ψ_1, χ_2 rational durch ψ_2 u. s. w. darstellbar. Es werden χ_1, χ_2, ... ganze Funktionen vom dritten Grade in z; setzt man dieselben gleich Null und löst die entstehenden Gleichungen

$$\chi_1 = 0, \quad \chi_2 = 0, \ldots,$$

so erhält man ihre Wurzeln; diese sind Funktionen dritten Grades in u. An Substitutionen, welche z. B. [00, 10, 20] ungeändert lassen, giebt es nur diejenigen drei, welche die Tripelelemente 00, 10, 20 untereinander umsetzen. Nach der Lösung der beiden Gleichungen, von denen die eine ψ, die andere z liefert, wird die Gleichung neunten Grades reduktibel. Sie zerfällt in drei Faktoren dritten Grades, welche, wie die Gruppe H_1 (§ 196) zeigt, Abel'sche Gleichungen liefern.

Die Berechnung der Wurzeln knüpft man besser an die Auflösung der beiden Gleichungen dritten Grades

$$\chi_1 = 0, \quad \chi_2 = 0,$$

von denen die erste die Werte von

1) $(u - x_{00})(u - x_{10})(u - x_{20})$,
2) $(u - x_{01})(u - x_{11})(u - x_{21})$,
3) $(u - x_{02})(u - x_{12})(u - x_{22})$,

und die zweite diejenigen von

4) $(u - x_{00})(u - x_{01})(u - x_{02})$,
5) $(u - x_{10})(u - x_{11})(u - x_{12})$,
6) $(u - x_{20})(u - x_{21})(u - x_{22})$.

Die Koefficienten dieser sechs Ausdrücke sind rational bekannt. Bestimmt man jetzt die grössten gemeinsamen Teiler von 1), 2), 3) mit 4), 5), 6), so erhält man alle neun Wurzeln

x_{00}, x_{10}, x_{20} als gemeinsame Teiler von 1) mit respektive 4), 5), 6),
x_{01}, x_{11}, x_{21} „ „ „ „ 2) „ „ 4), 5), 6),
x_{02}, x_{12}, x_{22} „ „ „ „ 3) „ „ 4), 5), 6).

Lehrsatz V. Die Tripelgleichung neunten Grades ist algebraisch lösbar. Nach der Auflösung einer Gleichung vierten und einer Gleichung dritten Grades zerfällt sie in drei rationale Faktoren dritten Grades, welche sämtlich Abel'sche Gleichungen sind. Die neun Wurzeln können durch die Auflösung einer Gleichung vierten und zweier Gleichungen dritten Grades gefunden werden.

§ 199. In enger Verbindung mit diesem steht das folgende Theorem:

Lehrsatz VI. Wenn eine irreduktible Gleichung neunten Grades so beschaffen ist, dass drei ihrer Wurzeln in einer durch die folgenden drei Gleichungen ausgedrückten Beziehung stehen

$$x_3 = \theta(x_1, x_2) = \theta(x_2, x_1), \quad x_1 = \theta(x_2, x_3) = \theta(x_3, x_2),$$
$$x_2 = \theta(x_3, x_1) = \theta(x_1, x_3),$$

in welchen θ eine rationale Funktion ihrer beiden Argumente bedeutet, so ist diese Gleichung algebraisch auflösbar.

Wir betrachten die Gruppe der betreffenden Gleichung. Sie ist transitiv; sie ersetzt die drei Wurzeln x_1, x_2, x_3 durch drei andere, zwischen denen dieselben Beziehungen stattfinden, wie zwischen x_1, x_2, x_3. Die neuen Wurzeln mögen x'_1, x'_2, x'_3 sein.

Stimmen die beiden Systeme in zwei Wurzeln überein, dann auch in der dritten; denn aus $x_1 = x'_1$, $x_2 = x'_2$ folgt

$$x'_3 = \theta(x'_1, x'_2) = \theta(x_1, x_2) = x_3,$$

und wären x'_3, x_3 nicht der Ausdruck für dieselbe Wurzel, so wäre die Gleichung, da sie gleiche Wurzeln besässe, nicht irreduktibel.

Ist x_4 eine von x_1, x_2, x_3 verschiedene Wurzel, so giebt es Substitutionen, welche x_1 in x_4 überführen; bleibt dabei keine der Wurzeln ungeändert, so erhält man ein neues System x_4, x_5, x_6; bleibt dagegen eine Wurzel, z. B. x_2, ungeändert, so erhält man als neues System x_2, x_4, x_7. Geht man in derselben Weise weiter, indem man die möglichen Wirkungen der Substitutionen untersucht, so erkennt man, dass alle Wurzeln sich in das Tripelsystem von neun Elementen einfügen, und dass die Gruppe der Gleichung daher eine Untergruppe der im vorigen Paragraphen besprochenen Gleichung ist. Sie ist also algebraisch lösbar (vergl. das fünfzehnte Kapitel).

Es ist bekannt*, dass die neun Inflexionspunkte, welche eine ebene Kurve dritter Ordnung besitzt, zu je drei und drei auf geraden

* O. Hesse: Crelle's Journal XXVIII, S. 68; XXXIV, S. 191. — Salmon: Crelle's Journal XXXIX, S. 365.

Linien liegen. Derartiger Linien giebt es zwölf, von denen je vier durch jeden Inflexionspunkt gehen. Je drei der Inflexionspunkte bilden also ein derartiges Tripel; sodass durch zwei Elemente desselben, die beliebig gewählt werden können, das dritte Element bestimmt ist. Die Abscissen oder die Ordinaten der neun Inflexionspunkte sind demnach die Wurzeln einer Gleichung neunten Grades mit Tripelcharakter, und die Gleichung ist algebraisch lösbar. Die Gleichung steht daher unter dem Geschlechte der in § 198 behandelten. Wir können sie aber auch in Beziehung zu den eben besprochenen setzen.

Es kann nämlich auch bewiesen werden, dass, wenn x_1, x_2, x_3 die Abscissen oder die Ordinaten dreier konjugierter Inflexionspunkte sind, dann

$$x_3 = \theta(x_1, x_2), \quad x_1 = \theta(x_2, x_3), \quad x_2 = \theta(x_3, x_1)$$

wird. Hierin bedeutet θ eine rationale in ihren beiden Argumenten symmetrische Funktion. Die Beweise für diese Eigentümlichkeiten übergehen wir, da dieselben fernliegenden Gebieten angehören.

Dreizehntes Kapitel.

Über die algebraische Auflösung der Gleichungen.

§ 200. In den letzten Kapiteln sind verschiedene Gleichungen behandelt worden, die infolge charakteristischer Beziehungen ihrer Wurzeln zu einander eine Anwendung der Theorie der Substitutionen ermöglichten. Jene Beziehungen waren von vornherein gegeben, und dieser Umstand ermöglichte unsere Schlüsse.

Bei allgemeinen Fragen dieser Art macht sich aber ein Zweifel geltend, der, wie schon früher angedeutet wurde, zuerst beseitigt werden muss, wenn eine Verwendung der Substitutionentheorie bei allgemeinen algebraischen Fragen gestattet werden soll. Die Theorie der Substitutionen knüpft lediglich an rationale Funktionen der Gleichungswurzeln an: treten daher bei der algebraischen Auflösung von algebraischen Gleichungen irrationale Funktionen der Wurzeln auf, so befinden wir uns auf einem Gebiete, in dem von Substitutionen überhaupt keine Rede mehr sein kann. Die Entscheidung der hierdurch aufgeworfenen prinzipiellen Frage kann natürlich nur auf algebraischem Wege möglich sein; die Anwendung der Substitutionentheorie würde eine petitio principii einschliessen. Es kann daher, um nur einen speziellen Fall hervorzuheben, ein Beweis für die

Unauflösbarkeit allgemeiner Gleichungen von höherem als dem vierten Grade durch rein substitutionen-theoretische Argumente nie geliefert werden.

§ 201. Bei algebraischen Fragen ist vorerst das Gebiet festzustellen, innerhalb dessen die zugehörigen Grössen als rational angesehen werden sollen.

Wir nehmen an, dass alle rationalen Funktionen gewisser gegebener Grössen $\Re'$, $\Re''$, $\Re'''$, ... mit ganzzahligen Koefficienten den Rationalitätsbereich $(\Re', \Re'', \Re''', \ldots)$ konstruieren.* Führt man unter irgend welchen Elementen dieses Bereiches die Operationen der Addition, Subtraktion, Multiplikation, Division, oder der Erhebung eines der Elemente in eine ganzzahlige Potenz aus, so wird das Resultat noch demselben Rationalitätsbereiche angehören.

Die Ausziehung von Wurzeln wird im allgemeinen solche Resultate geben, welche ausserhalb des Rationalitätsbereiches liegen. Wir können uns bei der Ausziehung von Wurzeln auf die Anwendung von Primzahlen als Wurzelexponenten beschränken, da eine $m.n^{\text{te}}$ Wurzel durch die m^{te} Wurzel aus einer n^{ten} ersetzt werden kann.

Alle diejenigen Funktionen von $\Re', \Re'', \Re''', \ldots$, welche nur durch ein- oder mehrfache Wurzelausziehungen aus den rationalen Funktionen erlangt werden können, fasst man unter den Begriff von algebraischen Funktionen zusammen, die zum Bereiche $(\Re', \Re'', \Re''', \ldots)$ gehören. Der erste Schritt von den rationalen zu den algebraischen Funktionen besteht demnach in der Ausziehung einer Wurzel mit Primzahlexponenten aus einer rationalen, ganzen oder gebrochenen Funktion $F_\nu(\Re', \Re'', \ldots)$. Die erhaltene Grösse sei V_ν, so dass

$$V_\nu^{p_\nu} = F_\nu(\Re', \Re'', \Re''', \ldots)$$

wird. Wir wollen unseren Rationalitätsbereich jetzt dadurch erweitern, dass wir ihm die Grösse V_ν zuordnen, adjungieren. Wir erhalten demnach von jetzt ab $(V_\nu; \Re', \Re'', \Re''', \ldots)$ als Rationalitätsbereich, d. h. es gelten uns alle ganzen oder gebrochenen Funktionen von V_ν, $\Re'$, $\Re''$, $\Re'''$, ... als rational. Dieser Bereich umfasst den früheren. Mit dieser Erweiterung geht eine Erweiterung der Reduktibilität Hand in Hand. Wenn z. B. in $x^{p_1} - \varphi(\Re', \Re'', \Re''', \ldots)$ die ganze Funktion φ so bestimmt ist, dass sie keine vollkommene p_1^{te} Potenz bildet, so ist im Bereiche $(\Re', \Re'', \Re''', \ldots)$ die Differenz $x^n - \varphi$ irreduktibel; nimmt man dagegen $V_\nu^{p_1} = \varphi$, so ist in dem Bereiche $(V_\nu; \Re', \Re'', \Re''', \ldots)$

* L. Kronecker: Berl. Ber. 1879, S. 205 flgg.; vergl. auch: arithm. Theorie d. algebr. Grössen.

die Differenz $x^n - \varphi$ zerlegbar, da sie den rationalen Faktor $x - V_\nu$ besitzt.

Den neuen Bereich können wir durch Ausziehung einer zweiten Wurzel mit Primzahlexponenten verlassen; wir bilden eine beliebige rationale Funktion $F_{\nu-1}(V_\nu; \mathfrak{R}', \mathfrak{R}'', \ldots)$ und bezeichnen die $p_{\nu-1}^{\text{te}}$ Wurzel mit $V_{\nu-1}$, so dass also

$$V_{\nu-1}^{p_\nu - 1} = F_{\nu-1}(V_\nu; \mathfrak{R}', \mathfrak{R}'', \ldots)$$

wird. V_ν ist nicht notwendig in $F_{\nu-1}$ enthalten, nur darf $F_{\nu-1}$ nicht in $V_\nu^{p_\nu - 1}$ oder $V_{\nu-1}$ im Rationalitätsbereich $(V_\nu; \mathfrak{R}', \mathfrak{R}'', \ldots)$ enthalten sein. Adjungieren wir jetzt $V_{\nu-1}$, so erhalten wir einen erweiterten Rationalitätsbereich, nämlich $(V_{\nu-1}, V_\nu; \mathfrak{R}', \mathfrak{R}'', \ldots)$. Ähnlich bilden wir weiter

$$V_{\nu-2}^{p_\nu - 2} = F_{\nu-2}(V_{\nu-1}, V_\nu; \mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots),$$

$$V_{\nu-3}^{p_\nu - 3} = F_{\nu-3}(V_{\nu-2}, V_{\nu-1}, V_\nu; \mathfrak{R}', \mathfrak{R}'', \ldots),$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$V_1^{p_1} = F_1(V_2, V_3, \ldots V_\nu; \mathfrak{R}', \mathfrak{R}'', \ldots);$$

dabei bedeuten die $F_1, F_2, \ldots F_{\nu-2}$ rationale Funktionen der eingeklammerten Grössen, die $p_1, p_2, \ldots p_{\nu-2}$ Primzahlen.

Ist also ein algebraischer Ausdruck vorgelegt, so kann man denselben nach dem angeführten Schema darstellen, indem man ihn genau so behandelt, wie man einen solchen, der nur Zahlengrössen enthält, bei der Ausrechnung behandeln würde.

§ 202. Die F_α können, wenn es nötig oder praktisch erscheinen sollte, derart umgeformt werden, dass sie in $V_{\alpha+1}, V_{\alpha+2}, \ldots V_\nu$ ganz und nur in den $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$ gebrochen sind. Hätte man z. B.

$$F_\alpha = \frac{G_0 + G_1 V_{\alpha+1} + G_2 V_{\alpha+1}^2 + \ldots}{H_0 + H_1 V_{\alpha+1} + H_2 V_{\alpha+1}^2 + \ldots},$$

wobei alle $G_0, G_1, \ldots; H_0, H_1, \ldots$ rational in $V_{\alpha+2}, V_{\alpha+3}, \ldots V_\nu$; $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$ sind, so möge mit $\omega_{\alpha+1}$ eine primitive $p_{\alpha+1}^{\text{te}}$ Einheitswurzel bezeichnet werden. Dann ist

$$\text{P)} \qquad \prod_{\lambda=0}^{p_{\alpha+1}-1} [H_0 + H_1 V_{\alpha+1} \omega_{\alpha+1}^\lambda + H_2 V_{\alpha+1}^2 \omega_{\alpha+1}^{2\lambda} + \ldots]$$

ganz und symmetrisch in den Wurzeln von

$$V_{\alpha+1}^{p_\alpha + 1} = F_{\alpha+1}(V_{\alpha+2}, \ldots V_\nu; \mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$$

und daher rational und ganz in den Koefficienten dieser Gleichung, d. h. in $F_{\alpha+1}$ und rational in $H_0, H_1, H_2, \ldots$, d. h. in $V_{\alpha+2}, \ldots V_\nu$; $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$ Daraus folgt, dass das Produkt P) eine rationale Funktion von $V_{\alpha+2}, \ldots V_\nu; \mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$ wird. Ferner wird

$$P_1) \qquad \prod_{\lambda=1}^{p_{\alpha+1}-1} [H_0 + H_1 V_{\alpha+1}\omega_{\alpha+1} + H_2 V_{\alpha+1}^2 \omega_{\alpha+1}^{2\lambda} + \ldots]$$

ganz in $V_{\alpha+1}$, rational in $V_{\alpha+2}, \ldots V_\nu$; $\Re', \Re'', \ldots$; und da es symmetrisch in den Wurzeln von

$$\frac{x^{p_{\alpha+1}}-1}{x-1} = x^{p_{\alpha+1}-1} + x^{p_{\alpha+1}-2} + \ldots + x + 1 = 0$$

ist, so fallen aus $P_1)$ die Potenzen von $\omega_{\alpha+1}$ heraus. Erweitert man daher den Ausdruck von F_α mit $P_1)$, so erhält man für den Nenner eine rationale Funktion von $V_{\alpha+2}, V_{\alpha+3}, \ldots V_\nu$; $\Re', \Re'', \ldots$, mit welcher man in die einzelnen Summanden des Zählers hineindividieren kann. Dadurch erhält man die Umwandlung

$$F_\alpha = J_0 + J_1 V_{\alpha+1} + J_2 V_{\alpha+1}^2 + \ldots,$$

worin alle Koefficienten $J_0, J_1, \ldots$ rationale Funktionen von $V_{\alpha+2}, V_{\alpha+3}, \ldots V_\nu$; $\Re', \ldots$ sind. Sollten in dieser Reihe höhere als die $(p_{\alpha+1}-1)^{\text{te}}$ Potenzen von $V_{\alpha+1}$ vorkommen, so kann man dieselben mittels der Definitionsgleichung für $V_{\alpha+1}$ wegen

$$V_{\alpha+1}^{p_{\alpha+1}} = F_{\alpha+1}, \quad V_{\alpha+1}^{p_{\alpha+1}+1} = F_{\alpha+1} \cdot V_{\alpha+1}, \quad V_{\alpha+1}^{p_{\alpha+1}+2} = F_{\alpha+1} \cdot V_{\alpha+1}^2, \ldots$$

entfernen, so dass

$$F_\alpha = J_0 + J_1 V_{\alpha+1} + J_2 V_{\alpha+2}^2 + \ldots + J_{p_{\alpha+1}-1} V_{\alpha+1}^{p_{\alpha+1}-1}$$

gesetzt werden kann. In zweiter Linie werden jetzt die einzelnen Koefficienten J ebenso umgeformt; sie können in $V_{\alpha+2}$ gebrochen sein; durch geeignete Erweiterung ihrer Bruchform wird jedes der J in eine rationale Funktion von $V_{\alpha+3}, \ldots V_\nu$; $\Re', \Re'', \ldots$ und in eine ganze bis zur $(p_{\alpha+2}-1)^{\text{ten}}$ Potenz aufsteigende ganze Funktion von $V_{\alpha+2}$ umgewandelt u. s. w.

Man kann die so erhaltenen Ausdrücke noch derart umgestalten, dass der Koefficient, welcher zur ersten Potenz der letzteingeführten algebraischen Irrationalität gehört, gleich der Einheit wird. Um den Beweis hierfür zu geben, muss aber zunächst ein Hilfssatz abgeleitet werden, welcher auch bei der Untersuchung der Form der Wurzeln, die auflösbaren Gleichungen eigentümlich ist, vielfache Verwendung finden wird.*

§ 203. Lehrsatz I. Sind $f_0, f_1, \ldots f_{p-1}$; F rationale Funktionen innerhalb eines bestimmten Rationalitätsbereiches,

* Abel, Oeuvres compl. II, 196, hat den Satz zuerst ausgesprochen; Herr L. Kronecker hat ihn in seiner vollen Bedeutung (Berl. Ber. 1879, S. 206) hingestellt.

so folgt aus dem gleichzeitigen Bestehen der beiden Gleichungen

$$\text{A)} \qquad f_0 + f_1 w + f_2 w^2 + \ldots + f_{p-1} w^{p-1} = 0,$$

$$\text{B)} \qquad w^p - F = 0,$$

entweder, dass eine der Wurzeln von B) demselben Rationalitätsbereich angehört, wie $f_0, f_1, \ldots f_{p-1}$; F, oder dass $f_0 = 0$, $f_1 = 0, \ldots f_{p-1} = 0$ ist.

Der grösste gemeinsame Teiler der Polynome in A) und B) wird als Koefficienten der höchsten Potenz von w die Einheit besitzen; er heisse

$$\varphi_0 + \varphi_1 w + \varphi_2 w^2 + \ldots + \varphi_{\nu-1} w^{\nu-1} + w^\nu.$$

Dieser wird, gleich Null gesetzt, ν Wurzeln von B) liefern; bezeichnet man daher eine von ihnen mit w_1 und eine primitive p^{te} Einheitswurzel mit ω_p, so sind alle diese ν Wurzeln in der Form

$$w_1, \ \omega_p^{\alpha} w_1, \ \omega_p^{\beta} w_1, \ \omega_p^{\gamma} w_1, \ \ldots$$

darstellbar. φ_0 ist, abgesehen vom Vorzeichen, ihr Produkt

$$\varphi_0 = \pm w_1^{\nu} \omega_p^{\delta}.$$

Da p eine Primzahl ist, so können wir zwei Zahlen u, v finden, für welche

$$pu + \nu v = 1$$

und also

$$\delta = pu\delta + \nu v\delta$$

wird. Trägt man diesen Wert von δ ein, so wird

$$\pm \varphi_0 = w_1^{\nu} \omega_p^{pu\delta + \nu v\delta} = w_1^{\nu} \omega_p^{\nu v\delta} = (w_1 \omega_p^{v\delta})^{\nu},$$

$$(\pm \varphi_0)^v = (w_1 \omega_p^{v\delta})^{1-pu} = w_1 \omega_p^{v\delta} \cdot w_1^{-pu} = w_1 \omega_p^{v\delta} \cdot F^{-u},$$

$$w_1 \omega_p^{v\delta} = F^u \cdot (\pm \varphi_0)^v;$$

eine Wurzel $w_1 \omega_p^{v\delta}$ von B) gehört also dem festgelegten Rationalitätsbereiche an.

Dies tritt nur dann nicht ein, wenn ein grösster gemeinsamer Teiler nicht vorhanden ist, trotzdem aber A), B) gleichzeitig bestehen, wenn also

$$f_0 = 0, \ f_1 = 0, \ \ldots f_{p-1} = 0$$

wird.

§ 204. Wir wollen von diesem Satze für die angedeutete Reduktion (§ 202, Schluss) von

$$F_\alpha = J_0 + J_1 V_{\alpha+1} + J_2 V_{\alpha+1}^2 + \ldots + J_{p_{\alpha+1}-1} V_{\alpha+1}^{p_{\alpha+1}-1}$$

Gebrauch machen. Ist $J_\varkappa$ irgend einer der Koefficienten $J_1, J_2, \ldots$ welcher nicht verschwindet, so nehmen wir

A_1) $$W_{\alpha+1} - J_\varkappa V_{\alpha+1}^{\varkappa} = 0,$$

B_1) $$V_{\alpha+1}^{p_{\alpha+1}} - F_{\alpha+1} = 0,$$

und setzen als Rationalitätsbereich

$$(V_{\alpha+2},\ V_{\alpha+3},\ \ldots\ V_\nu;\ \mathfrak{R}',\ \mathfrak{R}'',\ \ldots;\ W_{\alpha+1})$$

fest. Dann ist zufolge des obigen Satzes entweder $W_{\alpha+1} = 0$, $J_\varkappa = 0$ oder

C_1) $$V_{\alpha+1} = R(W_{\alpha+1},\ V_{\alpha+2},\ \ldots\ V_\nu;\ \mathfrak{R}',\ \mathfrak{R}'',\ \ldots).$$

Die erste der beiden Annahmen steht im Widerspruch zu den Voraussetzungen. Es muss daher die zweite giltig sein; folglich kann man in den Ausdruck von F statt $V_{\alpha+1}$ die Funktion $W_{\alpha+1}$ einführen, welche so beschaffen ist, dass $(V_{\alpha+1},\ V_{\alpha+2},\ \ldots\ V_\nu;\ \mathfrak{R}',\ \mathfrak{R}'',\ \ldots)$ und $(W_{\alpha+1},\ V_{\alpha+2},\ \ldots\ V_\nu;\ \mathfrak{R}',\ \mathfrak{R}'',\ \ldots)$ denselben Rationalitätsbereich konstituieren, wie aus A_1) und C_1) folgt. Es wird zudem

$$W_{\alpha+1}^{p_{\alpha+1}} = J_\varkappa^{p_{\alpha+1}} V_{\alpha+1}^{\varkappa p_{\alpha+1}} = \Phi_{\alpha+1}(V_{\alpha+2},\ V_{\alpha+3},\ldots V_\nu;\ \mathfrak{R}',\ \mathfrak{R}'',\ldots),$$

so dass, wenn man an Stelle von B_1) diese Definitionsgleichung in die Reihe der Irrationalitäten einführt, die Werte $V_\alpha,\ V_{\alpha-1},\ \ldots\ V_1$ nicht geändert werden, und man setzen kann

$$F_\alpha = J_0 + W_{\alpha+1} + L_2 W_{\alpha+1}^2 + L_3 W_{\alpha+1}^3 + \ldots + L_{p_{\alpha+1}-1} W_{\alpha+1}^{p_{\alpha+1}-1}.$$

Die Bestimmung der Koefficienten geschieht durch

$$W_{\alpha+1}^{\lambda} = J_\varkappa^{\lambda} V_{\alpha+1}^{\varkappa\lambda}.$$

Ist jetzt

$$\varkappa\lambda = q_\lambda p_{\alpha+1} + \lambda' \quad (\lambda' < p_{\alpha+1})$$

wo $q_\lambda p_{\alpha+1}$ das grösste in $\varkappa\lambda$ enthaltene Vielfache von $p_{\alpha+1}$ bedeutet, so wird

$$W_{\alpha+1}^{\lambda} = (J_\varkappa^{\lambda} F_{\alpha+1}^{q_\lambda}) V_{\alpha+1}^{\lambda'},$$

$$J_{\lambda'} V_{\alpha+1}^{\lambda'} = \frac{J_{\lambda'}}{J_\varkappa^{\lambda} F_{\alpha+1}^{q_\lambda}} W_{\alpha+1}^{\lambda} = L_\lambda W_{\alpha+1}^{\lambda}.$$

Da die Reste von

$$\varkappa,\ 2\varkappa,\ 3\varkappa,\ \ldots\ (p_{\alpha+1}-1)\varkappa \pmod{p_{\alpha+1}}$$

sämtlich unter einander verschieden sind, so liefert diese Methode völlig eindeutige Bestimmungen für die L.

§ 205. Wir gehen jetzt zu der Form der Wurzeln algebraisch auflösbarer Gleichungen über. Gegeben sei die Gleichung

1) $$f(x) = 0,$$

welche algebraisch auflösbar sein soll. Es heisst dies: von dem Rationalitätsbereiche $(\mathfrak{R}',\ \mathfrak{R}'',\ \mathfrak{R}''',\ \ldots)$ aus, in welchem sich jedenfalls die Koefficienten der Gleichung 1) befinden, kann man durch algebraische Operationen, also durch Addition und Subtraktion, Multi-

plikation und Division, Potenzieren und Radizieren mit Primzahlexponenten, die aber nur in endlicher Zahl zur Anwendung kommen, zu den Wurzeln von $f(x)=0$ gelangen. Eine dieser Wurzeln ist daher durch ein Schema darstellbar:

$$V_{\nu}^{p_\nu} = F_\nu(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots),$$
$$V_{\nu-1}^{p_\nu-1} = F_{\nu-1}(V_\nu; \mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots),$$
$$V_{\nu-2}^{p_\nu-2} = F_{\nu-2}(V_{\nu-1}, V_\nu; \mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$V_1^{p_1} = F_1(V_2, V_3, \ldots V_\nu; \mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots);$$
$$x_0 = G_0 + G_1 V_1 + G_2 V_1^2 + \ldots + G_{p_1-1} V_1^{p_1-1},$$

wo die $G_0, G_1, \ldots G_{p-1}$ ganze Funktionen von $V_2, V_3, \ldots V_\nu$ und rationale Funktionen von $\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots$ sind. G_1 kann gleich Eins angenommen werden (§ 204).

Durch Potenzieren und durch Reduktion der Potenzen von V_1, welche einen Exponenten $> p_1 - 1$ haben, kann man für jedes ν zu

$$x_0^\nu = G_0^{(\nu)} + G_1^{(\nu)} V_1 + G_2^{(\nu)} V_1^2 + \ldots + G_{p_1-1}^{(\nu)} V_1^{p_1-1}$$

gelangen. Setzt man diese Werte für $x_0, x_0^2, \ldots x_0^n$ in 1) ein, so entsteht

A) $$f(x_0) = H_0 + H_1 V_1 + H_2 V_1^2 + \ldots + H_{p_1-1} V_1^{p_1-1} = 0,$$

und andrerseits ist die Definitionsgleichung von V_1

B) $$V_1^{p_1} - F_1(V_2, V_3, \ldots) = 0.$$

Wendet man auf A), B) den Lehrsatz I) an, so treten zwei Möglichkeiten auf: entweder ist eine Wurzel von B) rational in dem Rationalitätsbereiche $(V_2, V_3, \ldots V_\nu; \mathfrak{R}', \mathfrak{R}'', \ldots)$, oder es sind

$$H_0 = 0, \; H_1 = 0, \; H_2 = 0, \ldots H_{p_1-1} = 0.$$

Beide Fälle können wirklich auftreten: im ersten Falle kann dann aber das Schema, mittels dessen man zu x_0 gelangt, dadurch vereinfacht werden, dass man die Gleichung

$$V_1^{p_1} = F_1(V_2, V_3, \ldots)$$

einfach unterdrückt und nur die p_1^{ten} Einheitswurzeln zum Rationalitätsbereiche hinzunimmt.

§ 206. Als Beispiel für diesen Fall diene die Gleichung dritten Grades

$$f(x) = x^3 - 3ax - 2b = 0.$$

Es ist

$$x_0 = \sqrt[3]{b + \sqrt{b^2 - a^3}} + \sqrt[3]{b - \sqrt{b^2 - a^3}}.$$

Diesen algebraischen Ausdruck kann man folgendermassen schematisieren

$$V_3^2 = b^2 - a^3,$$
$$V_2^3 = b + V_3,$$
$$V_1^3 = b - V_3;$$
$$x_0 = V_2 + V_1.$$

Dann wird der Ausdruck von $f(x_0)$ folgender sein

$$\tfrac{1}{3} f(x_0) = -a V_2 + (V_2^2 - a) V_1 + V_2 . V_1^2 = 0;$$

vergleicht man dies mit $V_1^3 - (b - V_3) = 0$

und bestimmt V_1 aus den beiden letzten Gleichungen, so erhält man

$$V_1 = \frac{a(b+V_3) - a^2 V_2 + (b - V_3) V_2^2}{a^2 + (b+V_3) V_2 - a V_2^2},$$

so dass also V_1 bereits in dem Rationalitätsgebiete $(V_2, V_3; a, b)$ enthalten ist. Macht man nun zuerst V_1 ganz in V_2 nach der Methode von § 202, so ergiebt sich wegen

$$[a^2 + (b+V_3) V_2 \omega - a V_2^2 \omega^2]\,[a^2 + (b+V_3) V_2 \omega^2 - a V_2^2 \omega] = 2b(b+V_3)(a+V_2^2),$$
$$[a^2 + (b+V_3) V_2 - a V_2^2]\,[2b(b+V_3)(a+V_2^2)] = [2b(b+V_3)]^2,$$
$$[a(b+V_3) - a^2 V_2 + (b - V_3) V_2^2]\,[2b(b+V_3)(a+V_2^2)] = 4ab^2 (b+V_3) V_2^2,$$

wo ω eine primitive dritte Einheitswurzel bedeutet,

$$V_1 = \frac{4ab^2(b+V_3) V_2^2}{4b^2 (b+V_3)^2} = \frac{a V_2^2}{b+V_3}.$$

Entfernt man V_3 aus dem Nenner durch Erweiterung mit $b - V_3$, so wird

$$V_1 = \frac{b - V_3}{a^2} V_2^2,$$

$$x_0 = V_2 + \frac{b - V_3}{a^2} V_2^2.$$

§ 207. Wir kehren zu den Betrachtungen von § 205 zurück und untersuchen den zweiten möglichen Fall. In

$$f(x_0) = H_0 + H_1 V_1 + H_2 V_1^2 + \ldots + H_{p_1 - 1} V_1^{p_1 - 1}$$

seien

$$H_0 = 0,\ H_1 = 0,\ H_2 = 0,\ \ldots\ H_{p_1 - 1} = 0.$$

Denken wir uns die Ausdrücke

$$x_\varkappa = G_0 + G_1 V_1 \omega_1^\varkappa + G_2 V_1^2 \omega_1^{2\varkappa} + \ldots G_{p_1 - 1} V_1^{p_1 - 1} \omega_1^{(p_1 - 1)\varkappa} \quad (\varkappa = 0, 1, \ldots p_1 - 1)$$

gebildet, in welchen ω_1 eine primitive Wurzel der Einheit sein soll, so folge

$$x_\varkappa^\nu = G_0^{(\nu)} + G_1^{(\nu)} V_1 \omega_1^\varkappa + G_2^{(\nu)} V_1^2 \omega_1^{2\varkappa} + \ldots + G_{p_1 - 1}^{(\nu)} V_1^{p_1 - 1} \omega_1^{(p_1 - 1)\varkappa},$$
$$f(x_\varkappa) = H_0 + H_1 V_1 \omega_1 + H_1 V_1^2 \omega_1^2 + \ldots + H_{p_1 - 1} V_1^{p_1 - 1} \omega_1^{(p_1 - 1)\varkappa}.$$

Unseren Voraussetzungen nach ist auch dieser Ausdruck $=0$, d. h. $x_\varkappa$ ist gleichfalls eine Wurzel von $f(x)=0$ für $\varkappa=0, 1, \ldots p_1-1$.

Im Beispiele der Gleichungen dritten Grades

$$x^3-3ax-2b=0$$

werden demnach, wenn wir durch die Wurzelform

$$x_0=V_2+\frac{b-V_3}{a^2}V_2^2$$

die erste der beiden Möglichkeiten beseitigen,

$$x_1=V_2\omega+\frac{b-V_3}{a^2}V_2^2\omega^2, \qquad \omega=\frac{-1+\sqrt{-3}}{2},$$
$$x_2=V_2\omega^2+\frac{b-V_3}{a^2}V_2^2\omega$$

die beiden anderen Wurzeln werden.

§ 208. Es sei nun, was nach § 204 erlaubt ist, $G_1=1$ gesetzt, dann findet man durch lineare Kombination der p_1 Gleichungen für $x_0, x_1, \ldots x_{p_1-1}$

$$x_0=G_0+G_1V_1+G_2V_1^2+\ldots+G_{p_1-1}V_1^{p_1-1},$$
$$x_1=G_0+G_1V_1\omega_1+G_2V_1^2\omega_1^2+\ldots+G_{p_1-1}V_1^{p_1-1}\omega_1^{p_1-1},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$x_{p_1-1}=G_0+G_1V_1\omega_1^{p_1-1}+G_2V_1^2\omega_1^{2(p_1-1)}+\ldots+G_{p_1-1}V_1^{p_1-1}\omega_1^{(p_1-1)^2},$$

$$G_1V_1=V_1=\frac{1}{p_1}\sum_{k=0}^{p_1-1}x_k\omega_1^{-k}.$$

Die Irrationalität V_1 ist demnach eine lineare Funktion der Wurzeln x_0, $x_1, \ldots x_{p_1-1}$, sobald man die Einheitswurzel ω_1 dem Rationalitätsbereiche zuordnet.

§ 209. Denkt man sich in dem Ausdrucke

$$y-\left[\frac{1}{p_1}\sum_{k=0}^{p_1-1}x_k\omega_1^{-k}\right]^{p_1}$$

alle Permutationen der die Gleichung $f(x)=0$ befriedigenden Wurzeln gemacht, so ist das Produkt aller dieser Ausdrücke eine ganze Funktion von y, deren Koefficienten symmetrische Funktionen der x und daher rationale Funktionen der $\mathfrak{R}'$, $\mathfrak{R}''$, $\mathfrak{R}'''$, ... sind.

Bezeichnet man diese Funktion mit $\varphi(y)$, so besitzt die Gleichung

$$\varphi(y)=0$$

die Wurzel

$$y_0 = \left(\frac{1}{p_1}\sum_{k=0}^{p_1-1} x_k \omega_1^{-k}\right)^{p_1} = V_1^{p_1} = F_1(V_2, V_3, \ldots V_\nu; \mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$$
$$= L_0 + L_1 V_2 + L_2 V_2^2 + \ldots + L_{p_2-1} V_2^{p_2-1},$$

wo wir L_1 wieder gleich Eins setzen dürfen. Man kann auf $\varphi(y) = 0$ mit der Wurzel y_0 dasselbe Verfahren anwenden, welches in den §§ 205, 207 auf $f(x) = 0$ mit der Wurzel x_0 angewendet wurde. Das Resultat wird sein, dass entweder V_2 in der Reihe V_ν, $V_{\nu-1}$, ... V_3, V_2, V_1 getilgt werden kann, oder, wenn man sich die Reihe bereits in dieser Weise geläutert denkt, dass

$$V_2 = \frac{1}{p_2}\sum_{k=0}^{p_2-1} y_k \omega_2^{-k}$$

wird, wo wir unter ω_2 eine primitive p_2^{te} Wurzel verstehen. Jedes der y_k entsteht aus y_0 durch gewisse Substitutionen unter den x_0, x_1, ... x_{n-1}; also ist V_2 eine ganze rationale Funktion von Wurzeln von $f(x) = 0$, falls man die Grössen ω_1, ω_2 zum Rationalitätsbereiche hinzunimmt.

In der dargelegten Weise fährt man fort und gelangt zu dem Resultate:

Lehrsatz II. Die einer auflösbaren Gleichung $f(x) = 0$ genügende explicite algebraische Funktion x_0 ist als ganze Funktion einer Reihe von Grössen

$$V_1, V_2, V_3, \ldots V_{\nu-1}, V_\nu$$

darstellbar, deren Koefficienten rationale Funktionen der Grössen $\mathfrak{R}'$, $\mathfrak{R}''$, ... sind; die Grössen V_i sind einerseits ganze Funktionen von Wurzeln der Gleichung $f(x) = 0$ und von Wurzeln der Einheit; andererseits werden sie durch eine Kette von Gleichungen

$$V_\alpha^{p_\alpha} = F_\alpha(V_{\alpha+1}, V_{\alpha+2}, \ldots V_\nu; \mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$$

bestimmt. In diesen Gleichungen sind $p_1, p_2, \ldots p_\nu$ Primzahlen; $F_1, F_2, \ldots F_\nu$ sind ganze Funktionen der eingeklammerten V und rationale Funktionen der Grössen $\mathfrak{R}', \mathfrak{R}'', \ldots$, welche den Rationalitätsbereich konstituieren.

§ 210. Dieser Satz gewährt die Möglichkeit der Verwendung von substitutionen-theoretischen Betrachtungen bei algebraischen Untersuchungen; er liefert den Beweis für den Fundamentalsatz:

Lehrsatz III. Die allgemeinen Gleichungen von höherem als dem vierten Grade sind nicht algebraisch auflösbar.

In der That, wären die n Grössen $x_1, x_2, \ldots x_n$, welche im Falle der allgemeinen Gleichung von einander unabhängig sind, algebraisch durch die $\Re', \Re'', \Re''', \ldots$ darstellbar, die wir als mit den Koefficienten der Gleichung zusammenfallend annehmen können, so würde die zuerst einzuführende Irrationalität V_ν die p_ν^{te} Wurzel aus einer rationalen Funktion der $\Re', \Re'', \Re''', \ldots$ sein. Bedenken wir, dass V_ν eine rationale Funktion der Wurzeln ist, so zeigt sich, dass V_ν, als eine p_ν-wertige rationale Funktion von $x_1, x_2, \ldots x_n$, deren p_ν^{te} Potenz symmetrisch wird, mit der Quadratwurzel aus der Diskriminante zusammenfallen und $p_\nu = 2$ sein muss (§ 57). Adjungieren wir diese Funktion $V_\nu = \sqrt{\Delta}$ dem Rationalitätsbereiche, so umfasst dasselbe alle ein- und alle zweiwertigen Funktionen der Wurzeln. Will man einen weiteren Schritt zur Lösung der Gleichung thun, was notwendig ist, wenn $n > 2$ angenommen wird, so müsste eine rationale Funktion $V_{\nu-1}$ der Wurzeln existieren, welche $2 . p_{\nu-1}$-wertig, deren $p_{\nu-1}^{\text{te}}$ Potenz dagegen zweiwertig ist. Eine solche Funktion giebt es aber für $n > 4$ nicht (§ 59); folglich lässt sich das Verfahren, welches zu den Wurzeln führen könnte, nicht weiter fortsetzen. Die allgemeinen Gleichungen von höherem als dem vierten Grade sind daher algebraisch nicht lösbar.

§ 211. Wir kehren zu der Form der Wurzel einer auflösbaren Gleichung

$$x_0 = G_0 + V_1 + G_2 V_1^{\,2} + \ldots + G_{p_1-1} V_1^{\,p_1-1}$$

zurück. Wir sahen bereits, dass die Einsetzung von

$$V_1 \omega_1^{\,k} \quad \text{statt} \quad V_1$$

auf neue Wurzeln der Gleichung führt. Diesen Satz kann man verallgemeinern. Wir setzen dabei voraus, dass das Schema, welches auf x_0 führt, schon nach Möglichkeit reduziert sei, so dass nicht etwa ein V_α bereits im Rationalitätsbereiche von $(V_{\alpha+1}, V_{\alpha+2}, \ldots V_\nu; \Re', \Re'', \Re''', \ldots)$ enthalten sei. Dann zeigen wir:

Lehrsatz IV. Multipliziert man in dem Ausdrucke von x_0 irgendwelche der Grössen $V_1, V_2, V_3, \ldots$ beliebig mit entsprechenden $p_1^{\text{ten}}, p_2^{\text{ten}}, p_3^{\text{ten}}$ Wurzeln der Einheit $\omega_1^{\,\varkappa}, \omega_2^{\,\lambda}, \omega_3^{\,\mu}, \ldots$, so wird das Resultat wiederum eine Wurzel der Gleichung $f(x) = 0$ sein, welcher x_0 genügt.

Für V_1 ist dies, wie soeben bemerkt wurde, bereits bewiesen. Bildet man

$$\prod_{k=0}^{p_1-1}(x-x_k)=\prod_{k=0}^{p_1-1}[x-(G_0+V_1\omega_1{}^k+G_2V_1{}^2\omega_1{}^{2k}+\ldots)]$$
$$=\alpha_0+\alpha_1V_2+\alpha_2V_2{}^2+\ldots+\alpha_{p_2-1}V_2{}^{p_2-1},$$

so wird dies ein Teiler von $f(x)$ sein; V_1 ist in diesem Ausdrucke verschwunden; die α_0, α_1 ... enthalten $x, V_3, V_4, \ldots V_r$; $\Re', \Re'', \ldots$ Nimmt man $(x; V_2, V_3, \ldots V_r; \Re', \Re'', \ldots)$ als Rationalitätsbereich, so giebt es innerhalb desselben Grössen $\alpha'_0, \alpha'_1, \ldots$, welche die Gleichung erfüllen

$A_1)$ $f(x;\Re',\Re'',\ldots)=(\alpha_0+\alpha_1V_2+\alpha_2V_2{}^2+\ldots)(\alpha'_0+\alpha'_1V_2+\alpha'_2V_2{}^2+\ldots).$

Setzt man diese Gleichung in die Form

$A_2)$ $$b_0+b_1V_2+b_2V_2{}^2+\ldots+b_{p_2-1}V_2^{p_2-1}=0$$

um und nimmt die Definitionsgleichung

B) $$V_2{}^{p_2}-F_2(V_3,\ldots V_r;\ \Re',\ldots)=0$$

zu Hilfe, so zeigt der erste Lehrsatz dieses Kapitels: entweder ist einer der Werte von V_2 rational in $(x, V_3, V_4, \ldots V_r; \Re', \ldots)$ oder es werden

$$b_0=0,\quad b_1=0,\quad b_2=0,\ \ldots\ b_{p_2-1}=0.$$

Die erste Möglichkeit muss ausgeschlossen werden; denn da V_2 wegen B) die unbestimmte Grösse x nicht enthält, so müsste es rational in $(V_3, V_4, \ldots V_r; \Re', \ldots)$ sein; und dies widerspricht den Festsetzungen über unser System der V.

Es tritt also der zweite Fall ein; d. h. $A_2)$ ist identisch für jedes V_2 erfüllt. Man kann daher V_2 mit $\omega_2{}^k$ in $A_2)$ oder in $A_1)$ multiplizieren. Es ist demnach

$A_0)$ $$f(x;\Re',\Re'',\ldots)$$
$$=(\alpha_0+\alpha_1V_2\omega_2{}^k+\alpha_2V_2{}^2\omega_2{}^{2k}+\ldots)(\alpha'_0+\alpha'_1V_2\omega_2{}^k+\alpha'_2V_2{}^2\omega_2{}^{2k}+\ldots);$$

und wie

$$\alpha_0+\alpha_1V_2+\alpha_2V_2{}^2+\ldots=\prod_{k=0}^{p_1-1}(x-x_k)=f_1(x;V_2,V_3,\ldots),$$

so wird auch

$$\alpha_0+\alpha_1V_2\omega_2{}^k+\alpha_2V_2{}^2\omega_2{}^{2k}+\ldots=f_1(x;V_2\omega_2{}^k,V_3,\ldots)$$

ein Faktor von $f(x;\Re',\Re'',\ldots)$ im Rationalitätsbereiche $(x; V_2, V_3, \ldots V_r; \Re', \Re'', \ldots)$ werden. Diesen letzten Faktor hätten wir erhalten, wenn wir bei x_0 statt V_2 überall in $G_0, G_1, G_2, \ldots$ eingesetzt hätten $V_2\omega_2{}^k$; benennt man den so entstehenden Wert für den Augenblick $x_0{}^{(k)}$, so ist auch $(x-x_0{}^{(k)})$ ein Faktor von $f(x)$ im Rationalitätsbereiche $(x; V_1, V_2, \ldots V_r; \Re', \Re'', \ldots)$, d. h. die vorgenommene Änderung hat uns eine neue Wurzel $x_0{}^{(k)}$ geliefert. Im ganzen erhalten wir so $p_1 . p_2$ Wurzeln von $f(x)=0$.

Wir bilden nun weiter

$$\prod_{k=0}^{p_3-1} f_1(x; V_2\omega_2^k, V_3, \ldots) = \beta_0 + \beta_1 V_3 + \beta_2 V_3^2 + \ldots + \beta_{p_3-1} V_3^{p_3-1};$$

dies ist im Rationalitätsbereiche $(x; V_3, V_4, \ldots)$ ein Teiler von $f(x)$; also giebt es in ihm auch Grössen $\beta'_0, \beta'_1, \beta'_2, \ldots$, welche die Gleichung

$$A'_1) \quad f(x; \mathfrak{R}', \mathfrak{R}'', \ldots) = (\beta_0 + \beta_1 V_3 + \beta_2 V_3^2 + \ldots)(\beta'_0 + \beta'_1 V_3 + \beta'_2 V_3^2 + \ldots)$$

befriedigen. Setzt man diese Gleichung in die Form

$$A'_2) \qquad c_0 + c_1 V_3 + c_2 V_3^2 + \ldots + c_{p_3-1} V_3^{p_3-1} = 0$$

um und nimmt die Definitionsgleichung

$$B'_2) \qquad V_3^{p_3} - F_3(V_4, \ldots V_r; \mathfrak{R}', \ldots) = 0$$

zu Hilfe, so zeigt der erste Lehrsatz dieses Kapitels: entweder ist einer der Werte von V_3 rational in $(x; V_4, V_5, \ldots V_r; \mathfrak{R}', \ldots)$, oder es sind

$$c_0 = 0, \; c_1 = 0, \; c_2 = 0, \; \ldots \; c_{p_3-1} = 0.$$

Die erste Möglichkeit muss ausgeschlossen werden; denn da V_3 wegen $B'_2)$ die unbestimmte Grösse x nicht enthalten kann, so müsste es rational in $(V_4, \ldots V_r; \mathfrak{R}', \ldots)$ sein; und dies widerspricht den Festsetzungen über unser System der V.

Es tritt somit der zweite Fall ein; $A'_2)$ wird identisch durch jedes V_3 erfüllt, also auch durch $V_3\omega_3^k$; dies letztere findet bei $A'_1)$ gleichfalls statt, da die Umwandlung von V_3 in $V_3\omega_3^k$ bei $A'_1)$ auf $A'_2)$ nur derart wirkt, dass bei ungeänderten $c_0, c_1, \ldots$ zu den Potenzen von V_3 noch Potenzen von ω_3 treten. Es ist demnach

$$A'_0) \qquad f(x; \mathfrak{R}', \mathfrak{R}'', \ldots)$$
$$= (\beta_0 + \beta_1 V_3\omega_3^k + \beta_2 V_3^2\omega_3^{2k} + \ldots)(\beta'_0 + \beta'_1 V_3\omega_3^k + \beta'_2 V_3^2\omega_3^{2k} + \ldots);$$

und wie

$$\beta_0 + \beta_1 V_3 + \beta_2 V_3^2 + \ldots = \prod_{k=0}^{p_1-1} f_1(x; V_2\omega_2^k, V_3, \ldots) = f_2(x; V_3, \ldots),$$

so wird auch

$$\beta_0 + \beta_1 V_3\omega_3^k + \beta_2 V_3^2\omega_3^{2k} + \ldots = f_2(x; V_3\omega_3^k, \ldots)$$

ein Faktor von $f(x; \mathfrak{R}', \mathfrak{R}'', \ldots)$ im Rationalitätsbereiche $(V_3, \ldots V_r; \mathfrak{R}', \mathfrak{R}'', \ldots)$ werden.

Wären wir bei der Produktbildung $f_1(x)$, $f_2(x)$ statt von $x - x_0$ von dem Faktor $x - x_0^{(k')}$ ausgegangen, der erhalten wird, wenn man in x_0 statt V_3 einsetzt $V_3\omega_3^{k'}$, so wäre in dem zugehörigen $f_1(x)$ jede Spur von V_1 und dann in $f_2(x)$ jede Spur von V_2 geschwunden; das zugehörige $f_2(x)$ wäre daher identisch mit dem obigen

$$f_2(x; V_3\omega_3{}^k, \ldots)$$

gewesen. Da dies ein Faktor von $f(x)$ ist, so ist $x_0{}^{(k)}$ eine Wurzel von $f(x) = 0$.

Diese Beweismethode lässt sich bis zu Ende fortsetzen.

§ 212. Hierbei ist noch dreierlei nachzuholen, was, um den Beweisgang im vorigen Paragraphen nicht zu unterbrechen, für diese Stelle aufgespart wurde.

Zuerst ist es nötig zu zeigen, dass z. B. mit $f_2(x; V_3, \ldots)$ auch das Produkt

$$f_3(x; V_4, \ldots) = \prod_{k=0}^{p_2-1} f_2(x; V_3\omega_3{}^k, \ldots)$$

ein Teiler von f wird. Dies steht fest, sobald die Irreduktibilität von f_2 in dem Rationalitätsbereiche $(V_3, V_4, \ldots; \mathfrak{R}', \mathfrak{R}'', \ldots)$ bewiesen ist. Gesetzt, es wäre $f_2(x)$ reduktibel und $\varphi_2(x; V_3, \ldots)$ einer seiner irreduktiblen Faktoren. Dann haben

$$\varphi_2(x; V_3, \ldots) = 0$$

und

$$f_1(x; V_2, V_3, \ldots) = 0$$

bei richtiger Wahl des irreduktiblen Faktors φ_2 eine Wurzel und die linken Seiten daher im Rationalitätsgebiete $(V_2, V_3, \ldots)$ einen Faktor gemeinsam. Setzen wir nun als bereits bekannt voraus, dass f_1 in diesem Gebiete irreduktibel ist, so wird f_1 ein Teiler von φ_2 sein, d. h. es wird

$$\varphi_2(x; V_3, \ldots) = f_1(x; V_2, V_3, \ldots)\,\psi_1(x; V_2, V_3, \ldots).$$

Nach der Methode des vorigen Paragraphen findet man, dass auch

$$f_1(x; V_2\omega_2{}^k, V_3, \ldots)$$

ein Teiler von φ_2 ist; also, da f_1 irreduktibel sein sollte, dass

$$\varphi_2(x; V_3, \ldots) = \prod_{k=0}^{p_2-1} f_1(x; V_2\omega_2{}^k, V_3, \ldots)\,.\,\chi(x; V_3, \ldots).$$

Das widerspricht dem Unstande, dass der Grad von φ_2 kleiner als der von f_2 ist.

Die Funktion f_2 ist also im Bereiche $(V_3, V_4, \ldots)$ rational, wenn es f_1 in $(V_2, V_3, \ldots)$ ist. So kann der Beweis bis auf die offenbar irreduktiblen Faktoren $x - x_\alpha$ zurückgedrängt werden.

§ 213. Ferner ist zu beachten, dass bei den Produktbildungen, z. B. bei

$$\prod_{k=0}^{p_2-1} f_1(x; V_2\omega_2{}^k, V_3, V_4, V_5, \ldots)$$

ausser V_2, welches notwendig in Wegfall kommen muss, auch noch andere V, z. B. V_3, V_4, verschwinden können; ja es wäre nicht einmal notwendig, dass diese gleichzeitig verschwindenden V unmittelbar dem V_2 vorhergehen müssen. Wie dem auch sei, verschwindet z. B. V_4 gleichzeitig mit V_2 in dem Produkte f_2, so heisst dies: es kommt im Produkte nur $V_4^{p_4}$, $V_4^{2p_4}$, ... vor; da diese Potenzen sich durch Überführung von V_4 in $V_4\omega_4^k$ nicht ändern, so ist demnach

$$\prod_{k=0}^{p_2-1} f_1(x; V_2\omega_2^k, V_3, V_4, \ldots) = \prod_{k=0}^{p_2-1} f_1(x; V_2\omega_2^k, V_3, V_4\omega_4^\lambda, \ldots);$$

wir sehen, dass diese Umwandlung von V_4 zu demselben Komplex von Wurzeln führt, den schon

$$\prod_{k=0}^{p_2-1} f_1(x; V_2\omega_2^k, V_3, V_4, \ldots) = 0$$

lieferte.

§ 214. Endlich ist zu erwähnen, dass die Art der Produktbildung ebensowenig wie die Anordnung der $V_r, V_{r-1}, \ldots V_1$ eine notwendig vorgeschriebene ist. Wenn z. B. in

$$x_0 = G_0 + G_1 V_1 + G_2 V_1^2 + \ldots + G_{p_1-1} V_1^{p_1-1}$$

der Ausdruck V_1 ein anderes V mit höherem Exponenten V_α nicht enthält, wo dann dieses allein in $G_0, G_1, \ldots G_{p_1-1}$ auftritt, dann kann man auch

$$x_0 = H_0 + H_1 V_\alpha + H_2 V_\alpha^2 + \ldots + H_{p_\alpha-1} V_\alpha^{p_\alpha-1}$$

setzen, und die erste Produktbildung in Beziehung auf

$$V_\alpha, \quad V_\alpha\omega_\alpha, \quad V_\alpha\omega_\alpha^2, \ldots V_\alpha\omega_\alpha^{p_\alpha-1}$$

durchführen. Der Gang der Beweise in den vorigen Paragraphen wird hierdurch gar nicht beeinflusst. Wir wollen ein V_1 oder ein V_α, welches in der angegebenen Art in einem algebraischen Ausdrucke vorkommt, ein äusseres Wurzelzeichen nennen, im Gegensatze zu den übrigen, welche innere Wurzeln sind.

§ 215. Nun fassen wir die Resultate der bisherigen Untersuchungen zusammen.

Lehrsatz V. Bildet man aus p_1 Faktoren $(x - x_k)$, welche so gewählt sind, dass das niedrigste äussere V_1 von x_0 in ihrem Produkte wegfällt, wobei gleichzeitig $V_2, V_3, \ldots V_{m_1-1}$ mit V_1 verschwinden mögen, das Produkt

$$f_1(x; V_{m_1}, \ldots) = \prod_{k=0}^{p_1-1} (x - x_k), \quad m_1 \geqq 2,$$

dann aus den p_{m_1} Faktoren $f_1(x; V_{m_1}\omega_{m_1}^k, \ldots)$ ein Produkt, in welchem V_{m_1} verschwindet, und auch $V_{m_1+1}, \ldots V_{m_2-1}$ noch verschwinden mögen:

$$f_2(x; V_{m_2}, \ldots) = \prod_{k=0}^{p_{m_2}-1} f_1(x; V_{m_1}\omega_{m_1}^k, \ldots), \qquad m_2 \geq m_1 + 1,$$

und fährt in dieser Weise fort, so erhält man, wenn alle Wurzelzeichen $V_1, V_2, \ldots V_r$ durch die Produktbildungen beseitigt sind, eine Funktion des Grades n

$$f(x; \mathfrak{R}', \mathfrak{R}'', \ldots),$$

welche, gleich Null gesetzt, x_0 zur Wurzel hat. Der Grad von $f(x)$ ist gleich

$$n = p_1 \cdot p_{m_1} \cdot p_{m_2} \cdots,$$

d. h. gleich dem Produkt der niedrigsten äusseren in x_0, f_1, $f_2, \ldots$ auftretenden Wurzelexponenten. Jedes f_α ist im Rationalitätsbereich $(V_{m_\alpha}, V_{m_\alpha+1}, V_r, \ldots; \mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$ irreduktibel.

Lehrsatz VI. Ist eine irreduktible Gleichung vom Primzahlgrade p algebraisch auflösbar, so wird der äussere Wurzelexponent gleich dem Grade p der Gleichung; ausser ihm giebt es keinen weiteren äusseren Exponenten; es wird das Gleichungspolynom folgendes sein:

$$f(x) = \prod_{k=0}^{p-1} (G_0 + V_1\omega_1^k + G_2 V_1^2 \omega_1^{2k} + \ldots + G_{p-1} V_1^{p-1} \omega_1^{k(p-1)}).$$

Lehrsatz VII. Treten in dem Ausdrucke von x_0 mehrere äussere Wurzelzeichen auf, so kommt das Produkt aller zugehörigen Exponenten als Faktor in n vor.

Denn in $\prod_k (x - x_k)$ kann ein V nur dann verschwinden, wenn alle seine Werte V, $V\omega$, $V\omega^2$, ... symmetrisch darin auftreten; bei einem äusseren V kommt dies nur vor, wenn wirklich die entsprechenden Faktoren für dieses V gebildet werden. Denn wenn V_1, V_α zwei äussere Wurzelzeichen sind, so wird man

$$\begin{aligned} x_0 &= G_0 + G_1 V_1 + G_2 V_1^2 + \ldots + G_{p_1-1} V_1^{p_1-1} \\ &= H_0 + H_1 V_\alpha + H_2 V_\alpha^2 + \ldots + H_{p_\alpha-1} V^{p_\alpha-1} \end{aligned}$$

setzen können. Enthielte nun das Produkt

$$\text{P)} \qquad \prod_{k=0}^{p_1-1} [x - (G_0 + G_1 V_1 \omega_1^k + G_2 V_1^2 \omega_1^{2k} + \ldots)]$$

kein V_α mehr, so würde es nach § 212 mit dem Produkte

$$\prod_{k=0}^{p_\alpha-1}[x-(H_0+H_1V_\alpha^k\omega_\alpha^k+H_2V_\alpha^2\omega_\alpha^{2k}+\ldots)]$$
$$=\prod_{k=0}^{p_\alpha-1}[x-(G_0^{(k)}+G_1^{(k)}V_1+G_2^{(k)}V_1^2+\ldots)]$$

übereinstimmen. Da sämtliche Faktoren beider Ausdrücke in x linear sind, so folgt aus dieser Übereinstimmung auch die der Faktoren, d. h. es wird z. B.

$$G_0+G_1V_1\omega_1^k+G_2V_1^2\omega_1^{2k}+\ldots=G_0^{(\varkappa)}+G_1^{(\varkappa)}V_1+G_2^{(\varkappa)}V_1^2+\ldots$$

oder

A) $$\Gamma_0+\Gamma_1V_1+\Gamma_2V_1^2+\ldots+\Gamma_{p_1-1}V_1^{p_1-1}=0.$$

Verbindet man hiermit die Definitionsgleichung von V_1, nämlich

B) $$V_1^{p_1}-F_1(V_2,V_3,\ldots V_\nu;\mathfrak{R}',\ldots)=0,$$

so würde nach dem ersten Lehrsatze entweder folgen, dass V_1 eine rationale Funktion von V_2, V_3, ... $\mathfrak{R}'$, $\mathfrak{R}''$, ... ist, und das ist unmöglich, oder dass

$$G_0=G_0^{(\varkappa)},\quad G_1\omega_1^k=G_1^{(\varkappa)},\quad G_2\omega_1^{2k}=G_2^{(\varkappa)},\ldots$$

wird. Da nun $G_\gamma^{(\varkappa)}$ aus G_γ entsteht, indem man V_α mit einem ω_α^λ multipliziert, so folgt durch Potenzieren mit p_1 leicht, es müsse

$$G_\gamma=K_\gamma V_\alpha^\gamma$$

sein, wo K_γ kein V_α mehr enthält, und ferner müsse $p_\alpha=p_1$ werden. Dann wird

$$x_0=K_0+K_1(V_1V_\alpha)+K_2(V_1V_\alpha)^2+\ldots+K_{p_1-1}(V_1V_\alpha)^{p_1-1}.$$

Da V_α ein äusseres Wurzelzeichen ist, kann man die Anordnung der V so treffen, dass $\alpha=2$ wird; demnach ist es möglich, auf V_3 sogleich $V_1.V_2$ folgen zu lassen, indem man als Definitionsgleichung

$$(V_1V_2)^{p_1}=F_1(V_3,\ldots)F_2(V_3,\ldots)$$

einführt. Solche Reduktionen können wir aber als von vornherein durchgeführt annehmen. Im Produkte P) kann daher V_α nicht verschwinden.

§ 216. Wir untersuchen jetzt die Änderungen, denen x_0 unterliegt, wenn man zu den Wurzeln V_2, V_3, ... V_{m_1-1}, welche bei der ersten Produktbildung wegfallen, irgendwelche entsprechenden p_2^{ten}, p_3^{ten}, ... $p_{m_1-1}^{\text{ten}}$ Einheitswurzeln als Faktoren hinzufügt. Es mögen

$$V_{m_1-1},\ V_{m_2-1},\ \ldots V_2,\ V_1;\ G_0,\ G_2,\ \ldots G_{p_1-1}$$

hierdurch in

$$v_{m_1-1},\ v_{m_2-1},\ \ldots v_2,\ v_1;\ g_0,\ g_1,\ \ldots g_{p_1-1}$$

übergehen und also

in
$$x_0 = G_0 + V_1 + G_2 V_1^2 + \ldots + G_{p_1-1} V_1^{p_1-1}$$
$$\xi_0 = g_0 + v_1 + g_2 v_1^2 + \ldots + g_{p_1-1} v_1^{p_1-1}.$$

Da nach § 213 hierbei die Gesamtheit der Wurzeln $x_0, x_1, \ldots x_{p_1-1}$ ungeändert bleibt, so wird das aus ξ_0 durch Einführung von v_1, $\omega_1 v_1$, $\omega_1^2 v_1$, ... gewonnene System von Wurzeln ξ_0, ξ_1, ξ_2, ... ξ_{p_1-1} mit jenem übereinstimmen. Wir können daher setzen

$$\begin{aligned}
g_0 + v_1 \quad + g_2 v_1^2 \quad + \ldots &= G_0 + V_1\omega_1' + G_2 V_1^2 \omega_1'^2 + \ldots,\\
g_0 + v_1\omega_1 + g_2 v_1^2 \omega_1^2 + \ldots &= G_0 + V_1\omega_1'' + G_2 V_1^2 \omega_1''^2 + \ldots,\\
g_0 + v_1\omega_1^2 + g_2 v_1^2 \omega_1^4 + \ldots &= G_0 + V_1\omega_1''' + G_2 V_1^2 \omega_1'''^2 + \ldots,\\
&\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

wobei ω_1', ω_1'', ω_1''', ... bis auf die Reihenfolge mit den Einheitswurzeln ω_1, ω_1^2, ω_1^3, ... übereinstimmen. Durch Addition dieser Gleichungen erhält man
$$g_0 = G_0;$$
es bleibt daher G_0 von allen in V_2, V_3, ... V_{m_1-1} ausgeführten Wertänderungen unberührt, d. h. G_0 ist rationale Funktion von V_{m_1}, V_{m_1+1}, ... $\mathfrak{R}'$, $\mathfrak{R}''$, .. allein. Im Falle von irreduktiblen Primzahlgleichungen, in denen $V_{m_1}, \ldots V_r$ nicht vorkommt, ist also G_0 rational im ursprünglichen Rationalitätsbereiche $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''', \ldots)$.

Weiter erhält man die Gleichung

$$\begin{aligned}
p_1 . v_1 = G_0(1 + \omega_1^{-1} + \omega_1^{-2} + \ldots) &+ V_1(\omega_1' + \omega_1''\omega_1^{-1} + \omega_1'''\omega_1^{-2} + \ldots)\\
&+ G_2 V_1^2(\omega_1'^2 + \omega_1''^2\omega_1^{-1} + \omega_1'''^2\omega_1^{-2} + \ldots)\\
&+ \ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

In dieser verschwindet der erste Summand der rechten Seite. Wir schreiben dieselbe Gleichung mit abkürzenden Bezeichnungen folgendermassen

$$\alpha) \qquad v_1 = \Omega_1 V_1 + \Omega_2 V_1^2 + \Omega_3 V_1^3 + \ldots$$

Die p_1^{te} Potenz derselben wird, wenn wir die Definitionsgleichungen berücksichtigen, folgende werden

$$\begin{aligned}
v_1^{p_1} = F_1(v_2, v_3, \ldots v_{m_1-1}; V_{m_1}, \ldots) &= [\Omega_1 V_1 + \Omega_2 V_1^2 + \ldots]^{p_1}\\
&= A_0 + A_1 V_1 + A_2 V_1^2 + \ldots
\end{aligned}$$

Nimmt man hierzu
$$V_1^{p_1} - F_1(V_2, V_3, \ldots V_r; \mathfrak{R}', \ldots) = 0,$$
so folgt aus dem ersten Lehrsatz, dass entweder

V_1 rational in $V_2, v_2; V_3, v_3; \ldots V_{m_1-1}, v_{m_1-1}; V_{m_1}; \ldots$

ist, oder dass
$$v_1^{p_1} = A_0, \quad A_1 = 0, \quad A_2 = 0, \ldots A_{p_1-1} = 0$$
wird.

Wir betrachten die erste Möglichkeit. Bei der rationalen Darstellung von V_1 durch $V_2, v_2, V_3, v_3, \ldots$ können nicht alle $v_2, v_3, \ldots$ fortfallen, da sonst V_1 rational in $V_2, V_3, \ldots V_{m_1}, \ldots$ wäre, was nicht angeht. Es wird demnach in

$$x_0 = R(V_1, V_2, \ldots V_\nu; \mathfrak{R}', \ldots) = R_1(V_2, v_2; V_3, v_3; \ldots)$$

ein äusseres V_α und ein äusseres v_β vorkommen $(\alpha, \beta < m_1)$. Im Rationalitätsbereiche $(V_{m_1}, V_{m_1+1}, \ldots V_\nu; \mathfrak{R}', \mathfrak{R}'', \ldots)$ ist x_0 eine Wurzel der irreduktiblen Gleichung

$$f_1(x; V_{m_1}, \ldots) = \prod_{k=0}^{p_1-1}(x - x_k) = 0$$

vom Primzahlgrade p_1. Da x_0 aber zwei äussere Wurzelzeichen V_α, v_β enthält, so ist dies nicht möglich (Lehrsatz VII). Die erste Annahme muss folglich verworfen werden.

Wir haben demnach anzunehmen, dass

$$A_0 = v_1^{p_1}, \quad A_1 = 0, \quad A_2 = 0, \quad A_3 = 0, \ldots$$

sei. Zu der Gleichung

$$A_0 = v_1^{p_1}$$

gelangte man durch Potenzierung von $\alpha)$. Dies ist nur möglich, wenn die rechte Seite von $\alpha)$ ein Monom in Beziehung auf V_1 ist. Daher hat $\alpha)$ die Form

$$\alpha') \qquad v_1 = \Omega_\lambda G_\lambda V_1^\lambda$$

und daraus erhält man

$$\xi_0 = g_0 + \Omega_\lambda G_\lambda V_1^\lambda + g_2(\Omega_\lambda G_\lambda V_1^\lambda)^2 + \ldots = G_0 + G_1 V_1 \omega_1' + G_2 V_1^2 \omega_1'^2 + \ldots$$

Der erste Lehrsatz zeigt, dass die Glieder mit gleichen Exponenten links und rechts einander gleich sein müssen; speziell wird

$$\Omega_\lambda G_\lambda V_1^\lambda = G_\lambda V_1^\lambda \omega_1'^\lambda,$$
$$\Omega_\lambda = \omega_1'^\lambda,$$
$$\alpha'') \qquad v_1 = \omega_1'^\lambda G_\lambda V_1^\lambda.$$

Lehrsatz VIII. Die Umwandlung von $V_2, V_3, \ldots V_{m_1-1}$ in $V_2\omega_2^\varkappa, V_3\omega_3^\lambda, \ldots V_{m_1-1}\omega_{m_1-1}^\mu$ führt $V_1^{p_1}$ in ein $(G_\lambda V_1^\lambda)^{p_1}$ über.

§ 217. Die durch $\alpha'')$ ausgesprochene Umwandlung führt $G_\alpha V_1^\alpha$ über in

$$g_\alpha v_1^\alpha = g_\alpha(\omega_1'^\lambda G_\lambda V_1^\lambda)^\alpha = g_\alpha \omega_1'^{\lambda\alpha} G_\lambda^\alpha V_1^{\lambda\alpha}.$$

Ist jetzt

$$\lambda\alpha = q_\alpha p_1 + \lambda_\alpha \qquad (0 < \lambda_\alpha < p_1),$$

so wird $G_\alpha V_1^\alpha$ in $G_{\lambda_\alpha} V_1^{\lambda_\alpha}$ übergeführt werden, wo λ_α durch die Kongruenz

$$\lambda_\alpha \equiv \lambda \,.\, \alpha \pmod{p_1}$$

bestimmt ist. Dieses Resultat weist darauf hin, eine primitive Wurzel $g \pmod{p_1}$ einzuführen und zu setzen

$$V_1 = R_0,\ G_g V_1^{\,g} = R_1,\ G_{g^2} V_1^{\,g^2} = R_2, \ldots$$

Dann wird die Reihe

$$R_0,\ R_1,\ R_2, \ldots R_{p_1-2}$$

mit der Reihe

$$V_1,\ G_2 V_1^{\,2},\ G_3 V_1^{\,3}, \ldots G_{p_1-1} V_1^{\,p_1-1}$$

übereinstimmen, und wir erhalten

$$x_0 = H_0 + R_0 + R_1 + R_2 + \ldots + R_{p_1-2}.$$

Die von uns betrachtete Wertänderung α'') der $V_2,\ V_3, \ldots V_{m_1-1}$ hat dann den Effekt

$$R_\alpha^{p_1} \quad \text{in} \quad R_{\alpha+\varkappa}^{p_1}$$

umzuwandeln, wo $\varkappa$ durch die Kongruenz definiert ist

$$g^\varkappa \equiv \varkappa \pmod{p_1},$$

und $\alpha + \varkappa$, wenn es grösser als $p_1 - 2$ sein sollte, durch seinen kleinsten nicht negativen Rest mod. $(p_1 - 1)$ zu ersetzen ist. Hält man dies fest, so kann man sagen, dass der Reihe nach durch α'')

I) $$R_0^{p_1},\ R_1^{p_1},\ R_2^{p_1}, \ldots R_{p_1-2}^{p_1}$$

in

II) $$R_\varkappa^{p_1},\ R_{\varkappa+1}^{p_1},\ R_{\varkappa+2}^{p_1}, \ldots R_{\varkappa+p_1-2}^{p_1}$$

übergeführt werden.

Die α-malige Anwendung derselben Wertänderungen ruft aus I)

III) $$R_{\alpha\varkappa}^{p_1},\ R_{\alpha\varkappa+1}^{p_1},\ R_{\alpha\varkappa+2}^{p_1}, \ldots R_{\alpha\varkappa+p_1-2}^{p_1}$$

hervor.

Existiert eine andere Wurzeländerung, durch welche $R_\gamma^{p_1}$ in $R_{\gamma+\mu}^{p_1}$ umgewandelt wird, so führt diese I) durch β-malige Anwendung in

IV) $$R_{\beta\mu}^{p_1},\ R_{\beta\mu+1}^{p_1},\ R_{\beta\mu+2}^{p_1}, \ldots R_{\beta\mu+p_1-2}^{p_1}$$

über.

Wendet man endlich die erste Operation α-mal und die zweite β-mal an, so gelangt man von I) zu

V) $$R_{\alpha\varkappa+\beta\mu}^{p_1},\ R_{\alpha\varkappa+\beta\mu+1}^{p_1},\ R_{\alpha\varkappa+\beta\mu+2}^{p_1}, \ldots R_{\alpha\varkappa+\beta\mu+p_1-2}^{p_1}.$$

In der Reihe I) sei nun $R_\varkappa^{p_1}$ dasjenige Glied, welches unter den durch Wurzeländerungen von $V_2,\ V_3, \ldots V_{m_1-1}$ aus $R_0^{p_1}$ ableitbaren den kleinsten Index hat; $R_\mu^{p_1}$ sei ein anderes, durch eine Wurzeländerung aus $R_0^{p_1}$ ableitbares.

Dann kann man durch α-malige Anwendung der Operation, welche zu $R_\varkappa^{p_1}$, und durch β-malige der Operation, welche zu $R_\mu^{p_1}$ führte, auf

$$R_{\alpha\varkappa+\beta\mu}^{p_1}$$

kommen. Bestimmt man α und β derart, dass

$$\alpha\varkappa+\beta\mu=\nu$$

den grössten gemeinsamen Teiler von $\varkappa$ und μ giebt, so erkennt man, dass $\nu=\varkappa$, also μ ein Vielfaches von $\varkappa$ ist. Alle von R_0^p aus erreichbaren Terme von I) sind also

$$R_0^{p_1},\ R_\varkappa^{p_1},\ R_{2\varkappa}^{p_1},\ \ldots\ R_{\left(\frac{p_1-1}{\varkappa}-1\right)\varkappa}^{p_1}.$$

Der letzte Term bestimmt sich durch die Bemerkung, dass eine nochmalige Anwendung derselben Operation von ihm zum ersten Term zurückführen muss. Wir sehen somit:

Lehrsatz IX. Die Anzahl der Werte, welche

$$R_0^{p_1}=V_1^{p_1}$$

dadurch annehmen kann, dass die Grössen $V_2,\ V_3,\ \ldots\ V_{m_1-1}$ mit willkürlichen $p_2^{\text{ten}},\ p_3^{\text{ten}},\ \ldots\ p_{m_1-1}^{\text{ten}}$ Einheitswurzeln $\omega_2^\varkappa,\ \omega_3^\lambda,\ \ldots\ \omega_{m_1-1}^\mu$ multipliziert werden, ist ein Teiler von p_1-1. Diese Anzahl ist gleich dem Grade der Gleichung

$$\varphi(V_1^{p_1})=0,$$

deren Koefficienten rational in $V_{m_1},\ V_{m_2},\ \ldots$ sind. Es giebt eine Art der Umwandlung von $V_2,\ V_3,\ \ldots\ V_{m_1-1}$, durch deren wiederholte Anwendung auf $V_1^{p_1}$ diese Grösse in alle ihre Werte übergeführt werden kann.

§ 218. Die Formel α'') aus § 216 zeigte, wie bei einer gewissen Umwandlung von $V_2,\ V_3,\ \ldots\ V_{m_1-1}$ der Term V_1 sich verhält. Er geht in

α'') $$v_1=\omega'_1 G_\lambda V_1^\lambda$$

über. Daraus kann man erkennen, in welche der Wurzeln $x_0,\ x_1,\ \ldots\ x_{p_1-1}$ hierbei x_0 verwandelt wird. Wir haben nämlich

$$\begin{aligned}
x_0&=G_0+V_1+G_2V_1^2+G_3V_1^3+\ldots\\
x_1&=G_0+V_1\omega_1+G_2V_1^2\omega_1^2+G_3V_1^3\omega_1^3+\ldots\\
x_2&=G_0+V_1\omega_1^2+G_2V_1^2\omega_1^4+G_3V_1^3\omega_1^6+\ldots\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

Diese Werte werden durch α'') in diejenigen derselben Reihe umgewandelt, in denen die Glieder

$$\omega'_1 G_\lambda V_1^\lambda,\quad \omega'_1\omega_1 G_\lambda V_1^\lambda,\quad \omega'_1\omega_1^2 G_\lambda V_1^\lambda,\ \ldots$$

vorkommen. Wäre z. B.

$$\omega_1^\alpha\omega_1'^\lambda=\omega_1^{\beta\lambda},$$

so würde durch α'') der Wert x_α in x_β umgewandelt werden.

§ 219. Wir untersuchen nun folgende Fälle:

I) Gesetzt, zwei Wurzeln x_α und x_β blieben bei der vorgenommenen Änderung ungeändert; dann wäre nach dem vorigen Paragraphen

$$\omega_1{}^\alpha . \omega_1'^\lambda = \omega_1{}^{\alpha\lambda}, \quad \omega_1{}^\beta . \omega_1'^\lambda = \omega_1{}^{\beta\lambda},$$

und daraus würde sich ergeben

$$\begin{aligned} (\alpha-\beta)\lambda &\equiv (\alpha-\beta) \pmod{p_1}, \\ \lambda &= 1, \\ \omega'_1 &= 1. \end{aligned}$$

Es würde also in α'') keine Einheitswurzel auftreten und mit x_α, x_β bliebe jede andere Wurzel ungeändert.

II) Gesetzt, eine Wurzel x_α bliebe ungeändert, während $x_{\alpha+1}$ in x_β übergehen soll. Dann hätte man

$$\omega_1{}^\alpha . \omega_1'^\lambda = \omega_1{}^{\alpha\lambda}, \quad \omega_1{}^{\alpha+1}\omega_1'^\lambda = \omega_1{}^{\beta\lambda};$$

hieraus folgt

$$\omega_1 = \omega_1{}^{(\beta-\alpha)\lambda},$$

oder nach Gauss'scher Bezeichnung

$$\lambda \equiv \frac{1}{\beta-\alpha} \pmod{p_1}.$$

Ginge nun x_γ über in x_δ, so wäre

$$\omega_1{}^\gamma . \omega_1'^\lambda = \omega_1{}^{\delta\lambda},$$

also

$$\omega_1{}^\gamma \omega_1{}^{\alpha\lambda-\alpha} = \omega_1{}^{\delta\lambda},$$

$$\begin{aligned} \delta\lambda &\equiv (\gamma-\alpha)+\alpha\lambda \pmod{p_1}, \\ \delta &\equiv (\beta-\alpha)(\gamma-\alpha)+\alpha \pmod{p_1}, \end{aligned}$$

so dass x_γ in $x_{(\beta-\alpha)(\gamma-\alpha)+\alpha}$ übergeht.

III) Gesetzt endlich, keine Wurzel bliebe ungeändert und dabei ginge x_β in x_γ und x_δ in x_ε über. Dann hätte man

$$\begin{aligned} \omega_1{}^\alpha \omega_1'^\lambda &\neq \omega_1{}^{\alpha\lambda} \quad (\alpha = 0, 1, 2, \ldots p_1-1), \\ \omega_1{}^\beta \omega_1'^\lambda &= \omega_1{}^{\gamma\lambda}, \quad \omega_1{}^\delta \omega_1'^\lambda = \omega_1{}^{\varepsilon\lambda}, \end{aligned}$$

und es folgte aus den letzten beiden Gleichungen

$$\begin{aligned} (\varepsilon-\gamma)\lambda &\equiv (\delta-\beta) \pmod{p_1}, \\ \lambda &\equiv \frac{\delta-\beta}{\varepsilon-\gamma} \pmod{p_1}; \end{aligned}$$

aus der ersten Gleichung ergiebt sich weiter, dass

$$\omega_1{}^\alpha \omega^{\gamma\lambda-\beta} \neq \omega_1{}^{\alpha\lambda},$$

$$\begin{aligned} (\alpha-\gamma)\lambda \text{ nicht } &\equiv \alpha-\beta \pmod{p_1}, \\ (\alpha-\gamma)(\delta-\beta) \quad \text{„} \quad &\equiv (\alpha-\beta)(\varepsilon-\gamma) \pmod{p_1} \\ \alpha(\varepsilon-\gamma-\delta+\beta) \quad \text{„} \quad &\equiv \gamma\delta-\beta\varepsilon \pmod{p_1} \quad (\alpha = 0, 1, 2, \ldots p_1-1). \end{aligned}$$

Dies letztere ist nur möglich, wenn gleichzeitig

$$\varepsilon \equiv \gamma + \delta - \beta, \quad \gamma\delta \text{ nicht } \equiv \beta\varepsilon \pmod{p_1};$$

die zweite dieser Bedingungen ist infolge der ersten von selbst befriedigt. Denn es ist

$$\beta\varepsilon \equiv \beta^2 - (\gamma+\delta)\beta + \gamma\delta \equiv (\beta-\gamma)(\beta-\delta) \text{ nicht } \equiv 0 \pmod{p_1}.$$

Lehrsatz X. Nimmt man in dem Ausdrucke für x_0 irgendwelche Umwandlungen von $V_2, V_3, \ldots V_{m_1-1}$ vor, welche derart beschaffen sind, dass zwei der Wurzeln $x_0, x_1, \ldots x_{p_1-1}$ sich nicht ändern, so bleiben sie sämtlich ungeändert; wenn nur x_α ungeändert bleibt, während $x_{\alpha+1}$ in x_β übergeht, so verwandelt sich jedes

$$x_\gamma \text{ in } x_{(\beta-\alpha)(\gamma-\alpha)+\alpha};$$

wenn keine der Wurzeln ungeändert bleibt und dabei x_α in x_β übergeht, dann verwandelt sich jedes

$$x_\gamma \text{ in } x_{\gamma+\beta-\alpha}.$$

§ 220. Eine wichtige Anwendung hiervon auf irreduktible auflösbare Gleichungen vom Primzahlgrade ist folgende: Es besteht kein $V_{m_1}, V_{m_1+1}, \ldots$ mehr; alle Umwandlungen, welche aus Änderungen von $V_2, V_3, \ldots V_{m_1-1}$ entstehen, sind gewissen Substitutionen unter den Wurzeln $x_0, x_1, \ldots x_{p_1-1}$ äquivalent; umgekehrt kann jede Substitution, welche unter den Wurzeln möglich ist, durch solche Umwandlungen von $V_2, V_3, \ldots V_{m_1-1}$ erreicht werden. Denn diese bieten die einzige Möglichkeit zu Vertauschungen der Wurzeln untereinander. Hieraus folgt, dass die Substitutionen der Gruppe G der Gleichung alle Wurzeln ungeändert lassen, sobald zwei Wurzeln ungeändert bleiben, dass sie also entweder alle p_1 Elemente umsetzen, oder $p_1 - 1$ oder gar keins. Im ersten Falle nehmen die Substitutionen die Gestalt an

$$s \equiv |\gamma \quad \gamma+\beta-\alpha| \equiv |\gamma \quad \gamma+\varkappa| \pmod{p_1},$$

im zweiten Falle die Gestalt

$$t \equiv |\gamma \quad (\beta-\alpha)(\gamma-\alpha)+\alpha| \equiv |\gamma \quad \lambda\gamma+\mu| \pmod{p_1}.$$

Wir gelangen also damit zu der Gruppe der Galois'schen Gleichungen.

Lehrsatz XI. Jede irreduktible auflösbare Gleichung eines Primzahlgrades ist eine Galois'sche Gleichung (im weiteren Sinne, so dass auch Abel'sche Gleichungen darunter verstanden sind).

Vierzehntes Kapitel.

Die Gruppe einer algebraischen Gleichung.

§ 221. Wir sahen bereits im neunten Kapitel § 152, dass jede spezielle Gleichung durch eine einzige zwischen ihren Koefficienten oder zwischen ihren Wurzeln stattfindende Beziehung völlig charakterisiert werden könne. Es sei etwa für $f(x) = 0$ diese Beziehung

$$\varphi(x_1, x_2, \ldots x_n) = 0.$$

Dann zeigte sich ebendaselbst, dass nicht eigentlich die Funktion, sondern dass die Gattung derselben das Charakteristische ist; demnach kann die zur Gattung gehörige Gruppe G vollkommen die Funktion φ vertreten. Unter den Wurzeln der Gleichung sind nur die zur Gruppe G gehörigen Substitutionen möglich. Es wurde der Hauptsatz bewiesen, welcher charakteristisch für die Gruppe ist:

Lehrsatz I. Alle im Rationalitätsbereiche von $f(x) = 0$ rational darstellbaren ganzen Funktionen der Wurzeln dieser Gleichung bleiben für die Gruppe G der Gleichung ungeändert, d. h. sie gehören zu ihrer Gattung oder stehen unter ihr; und umgekehrt lassen sich alle für die Substitutionen der Gruppe G ungeändert bleibenden Funktionen rational ausdrücken.

Wir werden wegen des genauen Zusammenhanges, der zwischen einer Gleichung und ihrer Gruppe besteht, die Ausdrücke „transitiv", „primitiv und imprimitiv", „einfach und zusammengesetzt" von den Gruppen auf Gleichungen übertragen. Es sollen also Gleichungen transitiv, primitiv oder imprimitiv, einfach oder zusammengesetzt heissen, wenn ihre Gruppen die entsprechenden Eigenschaften besitzen; umgekehrt werden wir die Benennung „auflösbar", welche der Theorie der Gleichungen entnommen ist, auf die Gruppen übertragen und von auflösbaren Gruppen als von solchen sprechen, deren Gleichung eine auflösbare ist. Da aber zu einer Gruppe unendlich viele Gleichungen gehören, so wird diese Einführung zu ihrer Rechtfertigung des Satzes bedürfen, dass die Auflösung aller zu derselben Gruppe gehörigen Gleichungen durch die einer einzigen unter ihnen gegeben wird. Dieser Satz wird später in der That bewiesen werden (Lehrsatz V).

Zuerst wollen wir versuchen, die Eigenschaften der Gruppen in äquivalente algebraische Eigenschaften der Gleichungen zu übertragen.

Wir wissen bereits aus § 154:

Lehrsatz II. Ist eine Gleichung irreduktibel, so ist ihre Gruppe transitiv und umgekehrt: ist die Gruppe einer Gleichung transitiv, so ist die Gleichung irreduktibel.

§ 222. Um die Frage zu beantworten, wie sich die Imprimitivität der Gruppe als Eigenschaft der Gleichung ausweist, erinnern wir an die Behandlung derjenigen Gleichungen, welche irreduktibel sind, und bei denen eine Wurzel eine rationale Funktion einer andern ist. Die Gleichung vom Grade $m.\nu$ zerlegte sich in ν Gleichungen vom Grade m, deren Koefficienten rational durch die Wurzeln einer Gleichung ν^{ten} Grades sich ausdrücken liessen (§ 170). Zu einem ähnlichen Resultate werden wir hier gelangen.

Angenommen, die Gruppe G der Gleichung $f(x)=0$ sei imprimitiv; dann können die Wurzeln derselben in ν Systeme von je m Wurzeln geteilt werden

$$x_{1,1},\ x_{1,2},\ \dots\ x_{1,m};\ x_{2,1},\ x_{2,2},\ \dots\ x_{2,m};\ \dots\ x_{\nu,1},\ x_{\nu,2},\ \dots\ x_{\nu,m} \quad (\nu.m=n)$$

derart, dass jede Substitution der Gruppe, welche eine Wurzel eines Systems in eine solche eines anderen umwandelt, alle Elemente des ersteren in alle des zweiten überführt. Wir betrachten jetzt als Resolvente eine beliebige symmetrische Funktion aller der Wurzeln, welche im ersten System enthalten sind,

$$1) \qquad y_1 = S(x_{1,1},\ x_{1,2},\ \dots\ x_{1,m}),$$

und wenden, um die Anzahl ihrer Werte kennen zu lernen, auf S alle Substitutionen von G an. Da die Gruppe G imprimitiv ist, so gehen alle Elemente $x_{1,1},\ x_{1,2},\ \dots\ x_{1,m}$ entweder nur in sich selber, oder gleichzeitig in die eines anderen Systems über; es giebt also nur noch $(\nu-1)$ Werte von y, nämlich

$$2) \qquad \left\{\begin{array}{l} y_2 = S(x_{2,1},\ x_{2,2},\ \dots\ x_{2,m}), \\ y_3 = S(x_{3,1},\ x_{3,2},\ \dots\ x_{3,m}), \\ \cdots\cdots\cdots\cdots \\ y_\nu = S(x_{\nu,1},\ x_{\nu,2},\ \dots\ x_{\nu,m}). \end{array}\right.$$

Folglich hängt y von einer Gleichung ν^{ten} Grades ab

$$3) \qquad \varphi(y)=0,$$

deren Koefficienten für alle Substitutionen von G ungeändert bleiben und daher nach Lehrsatz I) rational bekannt sind. Ist $\varphi(y)=0$ gelöst, d. h. sind alle ihre Wurzeln $y_1,\ y_2,\ \dots\ y_\nu$ bekannt, so kennt man auch alle symmetrischen Funktionen, welche aus den Wurzeln der einzelnen

Systeme gebildet werden können. Bezeichnet man insbesondere die elementaren symmetrischen Funktionen von $x_{\alpha,1}, x_{\alpha,2}, \ldots x_{\alpha,n}$ mit

$$S_1(y_\alpha),\ S_2(y_\alpha),\ \ldots\ S_m(y_\alpha),$$

so wird

4) $$x^m - S_1(y_\alpha)\,x^{m-1} + S_2(y_\alpha)\,x^{m-2} - \ldots \pm S_m(y_\alpha) = 0$$

die Gleichung, von welcher die Grössen $x_{\alpha,1}, x_{\alpha,2}, \ldots x_{\alpha,n}$ abhängen. Daher entsteht $f(x)=0$ durch die Elimination von y aus 3) und 4) und es wird

$$f(x) \equiv \prod_{\alpha=1}^{\nu} [x^m - S_1(y_\alpha)\,x^{m-1} + S_2(y_\alpha)\,x^{m-2} - \ldots \pm S_m(y_\alpha)] = 0.$$

Geht man umgekehrt von diesem letzteren Ausdrucke, dem Eliminationsresultat von y aus 3) und 4) aus, so ist die zu $f(x)=0$ gehörige Gruppe imprimitiv, falls 3) und 4) als irreduktibel vorausgesetzt werden. Denn wir bilden zuerst eine symmetrische Funktion der Wurzeln von 4); diese ist rational in y_α. Wir können sie daher, unter F eine rationale Funktion verstehend, gleich $F(y_\alpha)$ setzen. Ferner bilden wir das Produkt

5) $$[u - F(y_1)]\,[u - F(y_2)] \ldots [u - F(y_\nu)]$$

für alle Wurzeln von 4). Dieses Produkt ist dann rational bekannt; denn seine Koefficienten sind symmetrisch in $y_1, y_2, \ldots y_\nu$ und also rational durch die Koefficienten von 3) ausdrückbar. Nach dem ersten Lehrsatze bleibt 5) somit für alle Substitutionen der Gruppe ungeändert; die Gruppe muss infolgedessen die symmetrischen Funktionen von $x_{\alpha,1}, x_{\alpha,2}, \ldots x_{\alpha,n}$ in die symmetrischen Funktionen eines anderen Systems umwandeln, d. h. imprimitiv sein.

Lehrsatz III. Die Gruppe einer Gleichung vom Grade $n = m\nu$, welche durch Elimination von y aus den beiden irreduktiblen Gleichungen

3) $$\varphi(y) \equiv y^\nu - A_1 y^{\nu-1} + \ldots = 0,$$

4) $$x^m - S_1(y)\,x^{m-1} + S_2(y)\,x^{m-2} - \ldots + S_m(y) = 0$$

entsteht, ist imprimitiv; und umgekehrt ist jede Gleichung, deren Gruppe imprimitiv ist, das Resultat einer derartigen Elimination.

§ 223. Die Eigenschaften einer Gleichung, deren Gruppe zusammengesetzt ist, treten nicht in so übersichtlicher Weise heraus, wie dies bei der Transitivität oder bei der Imprimitivität der Gruppe der Fall ist. Man kann jedoch das Problem der Gleichungslösung durch ein anderes, ihm äquivalentes ersetzen, bei dem auch die

Eigenschaft der Zusammensetzung oder der Einfachheit ihrer Gruppe leicht übersehbare Einwirkung auf die Gleichung selbst haben.

Wir brauchen nämlich an die Stelle der allgemeinen Gleichung

6) $$f(x) = 0$$

nur diejenige zu setzen, welche ihre Galois'sche Resolvente liefert

7) $$F(\xi) = 0,$$

um das Gewünschte zu erhalten. $F(\xi)$ ist irreduktibel.

Wir wollen deshalb zuerst diese letztere Gleichung und ihre Eigenschaften einer genaueren Untersuchung unterziehen.

Ist eine allgemeine Gleichung 6) gegeben, so existiert eine lineare mit Hilfe von n unbestimmten Parametern gebildete Funktion der Wurzeln von 6)

8) $$\xi_1 = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n,$$

welche $n!$ Werte besitzt, so dass jede Substitution der zu 6) gehörigen symmetrischen Gruppe G von $x_1, x_2, \ldots x_n$ einen anderen Wert

$$\xi_1, \xi_2, \xi_3, \ldots \xi_{n!}$$

hervorruft. Diese durch G hervorgerufenen Umsetzungen zwischen $\xi_1, \xi_2, \ldots \xi_{n!}$ bilden eine Gruppe unter den $n!$ Elementen ξ, welche wir mit Γ bezeichnen wollen. Γ ist einstufig isomorph zu G; es ist die Gruppe von 7). Γ hat die Eigenschaft, dass ihre Ordnung ihrem Grade gleich ist, was entweder aus ihrer Bildung oder auch daraus geschlossen werden kann, dass alle ξ durch jedes beliebige unter ihnen rational darstellbar sind. Die Gleichung 7), welche identisch mit

7') $$(\xi - \xi_1)(\xi - \xi_2) \ldots (\xi - \xi_{n!}) = 0$$

ist, bedarf deshalb zu ihrer vollkommenen Lösung nur einer einzigen Wurzel.

Die Lösung von 7) ist äquivalent mit derjenigen von 6).

Es fragt sich, wie sich diese Verhältnisse modifizieren, wenn man von der allgemeinen Gleichung 6) zu einer speziellen übergeht. Eine jede solche wird durch die Hinzunahme einer einzigen Relation unter den Wurzeln

9) $$\varphi(x_1, x_2, \ldots x_n) = 0$$

charakterisiert. φ mag zur Gruppe G der Ordnung r gehören. Dann dürfen unter den Wurzeln nur diejenigen Substitutionen angewendet werden, welche zu G gehören. Denn wenn eine Substitution gestattet wäre, welche φ in

$$\varphi'(x_1, x_2, \ldots x_n) = 0$$

änderte, wo φ' von φ verschieden ist, so wären auch alle Funktionen von

$$\alpha\varphi(x_1, x_2, \ldots x_n) + \beta\varphi'(x_1, x_2, \ldots x_n)$$

rational bekannt. Der hierdurch bestimmte Rationalitätsbereich wäre umfassender als der durch 9) gegebene. Folglich würde 9) nicht alle Beziehungen, die zwischen den Wurzeln bestehen, in sich schliessen.

Man kann nun auf zweierlei Arten zu der Resolvente unserer besonderen Gleichung kommen. Entweder man geht von

8) $$\xi_1 = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$$

aus, wendet auf ξ_1 alle r Substitutionen von G an, erhält

$$\xi_1, \xi_2, \xi_3, \ldots \xi_r$$

und bildet die Resolvente r^{ten} Grades

10) $$F_1(\xi) \equiv (\xi - \xi_1)(\xi - \xi_2)\ldots(\xi - \xi_r) = 0;$$

oder man geht von dem fertigen Ausdrucke für $F(\xi)$ aus, der unter 7), 7') aufgestellt war, beachtet, dass derselbe reduktibel wird, wenn man 9) adjungiert, und dass $F_1(\xi)$ einer seiner irreduktiblen Teiler wird. Die übrigen Teiler werden, ebenso wie $F_1(\xi)$ vom Grade r; sie unterscheiden sich nur durch die Konstanten α von einander. Jeder entsteht durch die Multiplikation aller Faktoren $(\xi - \xi_\alpha)$, welche durch die Anwendung der Gruppe G aus einem einzigen unter ihnen entstehen. Die Gruppe von $F_1(\xi) = 0$, als Gruppe unter den ξ aufgefasst, ist vom Grade und der Ordnung r; sie ist einstufig isomorph zu der Gruppe G des Grades n und der Ordnung r, welche zu φ gehört.

Die Gruppen aller Faktoren $F_1(\xi), \ldots$ von $F(\xi)$ sind daher nur durch die Bezeichnung von einander unterschieden.

Lehrsatz IV. Ist eine spezielle Gleichung $f(x) = 0$ durch die Gattung von

9) $$\varphi(x_1, x_2, \ldots x_n) = 0$$

charakterisiert, deren Gruppe G die Ordnung r hat, so zerfällt die allgemeine Galois'sche Resolvente in $\varrho = \frac{n!}{r}$ Faktoren

10) $$F_1(\xi) = 0,$$

deren jeder als Galois'sche Resolvente der speziellen Gleichung gelten kann. Alle Wurzeln von 10) sind rationale Funktionen jeder einzelnen; durch diese können alle Wurzeln von $f(x) = 0$ ausgedrückt werden. Der Übergang von $f(x) = 0$ zu $F_1(\xi) = 0$ ist identisch mit demjenigen von G zu der einstufig isomorphen Gruppe Ω (§ 122).

Da bei der Bildung von 10) nur die Gruppe, nicht die spezielle Natur von 9) entscheidend ist, so gehört dieselbe Resolvente zu allen

Gleichungen, welche durch Funktionen derselben Gattung charakterisiert sind. Ist eine von diesen gelöst, so ist $x_1, x_2, \ldots x_n$ und damit ξ_1 bekannt; also ist 10) gelöst und damit jede andere derartige Gleichung. Wir erhalten also den Beweis für den in § 221 ausgesprochenen Satz:

Lehrsatz V. Sind zwei Gleichungen $f_1(x) = 0$, $f_2(x) = 0$ durch Wurzelbeziehungen $\varphi_1 = 0$ respektive $\varphi_2 = 0$ charakterisiert, welche zu derselben Gattung gehören, so zieht die Auflösung der einen diejenige der anderen nach sich.

§ 224. Wir haben in früheren Kapiteln Fälle behandelt, bei denen in der That derartige Wurzelbeziehungen entweder direkt gegeben oder leicht aus der gestellten Aufgabe herauszulesen waren. Häufig liegt die Sache aber so, dass nicht direkt eine bekannte Funktion $\psi(x_1, \ldots x_n)$ zur Adjungierung vorliegt, sondern dass ψ implicit, als Wurzel einer Gleichung, auftritt, welche als auflösbar angesehen wird. So ist z. B. bei dem Problem der algebraischen Auflösung von Gleichungen die Hilfsgleichung von der einfachen Form

$$y^p - A(x_1, \ldots x_n) = 0;$$

hierbei wird y als bekannt angesehen, d. h. wir erweitern den Rationalitätsbereich von $f(x) = 0$ derart, dass wir eine jede rationale Funktion der Wurzeln ihm adjungieren, sobald eine Potenz dieser Funktion dem Bereiche angehört. Von einer wirklichen Lösung der Gleichung ist nicht die Rede.

Es erscheint angemessen, dass, wenn man eine irreduktible Hilfsgleichung als auflösbar ansieht, nicht eine Wurzel ψ derselben zu $f(x) = 0$ adjungiert wird, sondern dass dies mit sämtlichen Wurzeln der Hilfsgleichung geschieht. Dies sind die verschiedenen Werte, welche $\psi(x_1, \ldots x_n) = \psi_1$ im Rationalitätsbereiche von $f(x) = 0$ annimmt. Denn um die Hilfsgleichung zu finden, der ψ_1 als Wurzel genügt, wenden wir auf ψ_1 alle r Substitutionen der Gruppe von G an und erhalten z. B. m von einander verschiedene Werte

$$11) \qquad \psi_1, \psi_2, \psi_3, \ldots \psi_m.$$

Die symmetrischen Funktionen derselben sind im Rationalitätsbereiche von $f(x) = 0$ bekannt; also auch die Koefficienten der Gleichung

$$12) \qquad g(\psi) \equiv (\psi - \psi_1)(\psi - \psi_2)\ldots(\psi - \psi_m) = 0,$$

und 12) ist die gesuchte Hilfsgleichung, deren Lösung als bekannt angesehen wird.

Nun ist die durch die Gruppe G respektive eine zu G gehörige Funktion $\varphi(x_1, \ldots x_m)$ charakterisierte Gleichung $f(x) = 0$ gegeben.

Ihr adjungieren wir alle Wurzeln von 12), oder, was dieselben Dienste leistet, die eine lineare Kombination jener m Wurzeln

$$\chi = \alpha_1\psi_1 + \alpha_2\psi_2 + \ldots + \alpha_m\psi_m.$$

Es fragt sich, wie daraufhin die Gruppe von $f(x) = 0$ sich gestaltet.

Die adjungierte Funktionengattung war vorher φ; jetzt ist sie

$$\varphi + \chi = \varphi + \alpha_1\psi_1 + \alpha_2\psi_2 + \ldots + \alpha_m\psi_m.$$

Die Gruppe war vorher G; jetzt ist es diejenige Untergruppe von G, welche gleichzeitig auch in den Gruppen von $\psi_1, \psi_2, \ldots \psi_m$ enthalten ist. Wir bezeichnen diese Gruppen von $\psi_1, \psi_2, \ldots \psi_m$ der Reihe nach mit

$$H_1, H_2, \ldots H_m.$$

Die grösste diesen m Gruppen gemeinsame Untergruppe sei K. Dann gehört K zur Funktion χ.

Wendet man nun auf die Reihe der $\psi_1, \psi_2, \ldots \psi_m$ die Substitutionen von G an, so reproduziert sich die Reihe bis auf ihre Anordnung; denn $\psi_1, \ldots \psi_m$ sind ja alle und nur diejenigen Werte, die aus ψ_1 durch Anwendung von G hervorgehen; also reproduziert sich auch die Reihe der $H_1, H_2, \ldots H_m$ bei Transformationen mit Substitutionen von G, und deshalb ändert sich K nicht, wenn man es durch G transformiert. Man hat also die Gleichung

$$G^{-1}KG = K.$$

Mit Γ bezeichnen wir weiter diejenige Untergruppe von G, welche in K enthalten ist; sie gehört demnach zu $\varphi + \chi$; sie charakterisiert die Gattung, welche zu $f(x) = 0$ nach der Adjunktion sämtlicher Wurzeln von 12) gehört. Wie K, so ist auch Γ mit G vertauschbar; Γ ist eine ausgezeichnete Untergruppe von G und zwar die umfassendste unter denjenigen, welche gleichzeitig in $H_1, H_2, \ldots H_m$ enthalten sind.

Hieraus ist noch zu schliessen, dass G eine zusammengesetzte Gruppe ist; doch findet dies nur statt, wenn sich Γ nicht auf die Einheit reduziert; denn eine ausgezeichnete Untergruppe, die gleich 1 ist, deutet noch nicht auf die Zusammensetzung einer Gruppe hin.

Andererseits erkennen wir, dass, wenn G einfach ist, Γ sich unbedingt gleich der Einheit ergeben wird; dann reduziert sich die Gruppe von $f(x) = 0$ durch die Lösung von 12) auf 1, d. h. es sind nach der Lösung von 12) alle Wurzeln von $f(x) = 0$ bekannt, oder auch: durch die Lösung von 12) wird $f(x) = 0$ gleichfalls gelöst. Dies liefert folgenden Satz:

Lehrsatz VI. Ist eine beliebige Gleichung $f(x)=0$ mit der Gruppe G gegeben und adjungiert man ihr sämtliche Wurzeln

11) $$\psi_1, \psi_2, \psi_3, \ldots \psi_m$$

einer irreduktiblen Gleichung m^{ten} Grades

12) $$g(\psi) \equiv \psi^m - A\psi^{m-1} + \ldots = 0,$$

deren Koefficienten rational im Rationalitätsbereiche von $f(x)$ und deren Wurzeln rationale Funktionen von $x_1, x_2, \ldots x_n$ sind, so reduziert sich G auf die höchste ausgezeichnete Untergruppe Γ von G, welche $\psi_1, \psi_2, \ldots \psi_m$ ungeändert lässt. Ist G eine einfache Gruppe, so wird $\Gamma = 1$. Nur wenn G zusammengesetzt ist, kann man durch Auflösung einer Hilfsgleichung die Gruppe auf eine von der Einheit verschiedene Untergruppe reduzieren und damit die Resolventengleichung in nicht lineare Faktoren zerlegen (vergl. § 196).

§ 225. Wir verweilen einen Augenblick bei diesen Resultaten. Ist die allgemeine Gleichung n^{ten} Grades $f(x)=0$ vorgelegt, so hat die zugehörige Gruppe G die Ordnung $r=n!$ und die Galois'sche Resolventengleichung den Grad $n!$ Die Gruppe ist zusammengesetzt; die einzige ausgezeichnete Untergruppe ist die alternierende (§ 84). Nimmt man als Resolvente

$$\psi_1 = \sqrt{\Delta},$$

wo Δ wie gewöhnlich die Diskriminante von $f(x)$ bedeutet, dann wird die Resolventengleichung

12′) $$\psi^2 - \Delta = 0$$

und Γ wird die alternierende Gruppe. Nach Adjungierung der beiden Wurzeln von 12′) zerfällt die vorher irreduktible Galois'sche Resolventengleichung in zwei gleichberechtigte Faktoren des Grades $\frac{1}{2}n!$, und die Resolvente

$$\xi = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$$

lässt jetzt nur noch Substitutionen zu, welche $\sqrt{\Delta}$ nicht ändern und also der alternierenden Gruppe angehören.

Für $n>4$ ist die alternierende Gruppe einfach. Gesetzt, es gäbe eine m-wertige Resolvente ψ, so hängen die Werte $\psi_1, \psi_2, \ldots \psi_m$ derselben von der Lösung einer Gleichung m^{ten} Grades ab. Durch die Adjungierung derselben, oder auch durch diejenige von

$$\chi = \beta_1\psi_1 + \beta_2\psi_2 + \ldots + \beta_m\psi_m$$

reduziert sich nach dem Lehrsatze VI) die Gruppe der Gleichung auf die identische Substitution 1. (Dies ist auch daraus ersichtlich, dass

1 die einzige Substitution ist, welche in den Gruppen von $\psi_1, \psi_2, \ldots \psi_m$ gleichzeitig auftritt.) Die Gleichung $f(x)=0$ ist demnach gelöst; denn es sind alle Funktionen bekannt, welche zur Gruppe 1 gehören oder unter ihr stehen. Unsere Untersuchungen aus dem sechsten Kapitel zeigen jedoch, dass hierbei eine Erniedrigung des Grades der aufzulösenden Gleichung nicht erzielt werden kann, da für $n>4$ die Anzahl m der Werte von ψ, wenn sie 2 übertrifft, grösser oder gleich n ist. Im letzteren Falle wird für $n \neq 6$ stets ψ in $(n-1)$ Elementen symmetrisch werden, so dass wir direkt $\psi = x_1$ setzen und die Resolventengleichung mit der ursprünglichen $f(x)=0$ identifizieren können.

Lehrsatz VII. Die allgemeine Gleichung n^{ten} Grades $(n>4)$ wird durch die Lösung einer beliebigen Resolventengleichung von höherem als dem zweiten Grade gelöst. Es giebt jedoch keine Resolventengleichungen, deren Grad grösser als 2 und kleiner als n wäre. Ist $n \neq 6$, so giebt es auch keine von der Gleichung $f(x)=0$ wesentlich verschiedene Resolventengleichungen n^{ten} Grades; bei $n=6$ giebt es eine solche.

Es möge ferner noch ein Resultat früherer Untersuchungen in die Form unserer jetzigen Anschauungen gekleidet werden:

Lehrsatz VIII. Die allgemeine Gleichung fünften Grades besitzt eine Resolventengleichung sechsten Grades.

§ 226. Wir kehren nach den beiläufigen Resultaten des vorigen Paragraphen auf den Lehrsatz VI) zurück und wenden uns zur Untersuchung der Gruppe der Gleichung

$$12) \qquad g(\psi) \equiv (\psi-\psi_1)(\psi-\psi_2)\ldots(\psi-\psi_m)=0,$$

deren Wurzeln $\psi_1, \psi_2, \ldots \psi_m$ sämtlich der Gleichung $f(x)=0$ adjungiert wurden.

Die Ordnung der Gruppe von 12) finden wir am einfachsten durch die Bemerkung, dass dieselbe gleich dem Grade der irreduktiblen Gleichung ist, welcher

$$\omega = \gamma_1\psi_1 + \gamma_2\psi_2 + \ldots + \gamma_m\psi_m$$

als Wurzel genüge leistet. Fassen wir ω als Funktion von $x_1, x_2, \ldots x_n$ auf, so stellt sich K als die Gruppe von ω heraus; Γ ist die umfassendste Untergruppe, welche K und G gemeinsam haben. Um also alle Werte zu erhalten, welche ω im Rationalitätsbereiche von $f(x)=0$ anzunehmen im stande ist, muss man G auf ω in Anwendung bringen; die Anzahl der verschiedenen Werte ist sodann gleich dem Quotienten aus den Ordnungen r von G und r' von Γ; wir setzen $\nu = \frac{r}{r'}$.

Man erkennt daraus, dass, wenn die Gruppe G einfach, Γ also von der Ordnung $r'=1$ ist, die Ordnung ν der Gruppe einer beliebigen Resolventengleichung mit derjenigen von $f(x)=0$ wiederum übereinstimmt, so dass also keinerlei Vereinfachung dadurch hervorgerufen wird.

Zur Gruppe von 12) selbst kommen wir durch die Überlegung, dass sie alle und nur solche Substitutionen unter den ψ enthält, welche die Natur von $f(x)=0$ nicht ändern; wendet man daher auf

11) $$\psi_1, \psi_2, \psi_3, \dots \psi_m$$

die Substitutionen von G an und fasst die Umstellungen der ψ als Substitutionen zwischen diesen Elementen auf, so bilden diese Substitutionen die Gruppe. Es sind jedoch nicht alle r so erhaltenen Substitutionen von einander verschieden; denn jede Substitution, die zu Γ gehört, lässt alle Elemente ψ an ihren Stellen. Auch hieraus folgt wieder die Ordnung der Gruppe von 12) gleich $\nu=\frac{r}{r'}$. Ebenso erkennt man, dass diese Gruppe r'-stufig isomorph zur Gruppe von $f(x)=0$ ist.

Lehrsatz IX. Ist G, die Gruppe von $f(x)=0$ von der Ordnung r; besitzt dieselbe eine ausgezeichnete Untergruppe Γ von der Ordnung r'; reduziert sich ferner G auf Γ, nachdem der Gleichung $f(x)=0$ sämtliche Wurzeln 11) von

12) $$g(\psi)=0$$

adjungiert sind, dann ist die Ordnung der Gruppe dieser letzteren Gleichung $\nu=\frac{r}{r'}$ und die Gruppe ist zu derjenigen von $f(x)=0$ r'-stufig isomorph.

Wir können der Gleichung 12) einen ganz speziellen Charakter durch passende Wahl der Resolvente verleihen.

Wir wählen als Resolvente eine zur ausgezeichneten Untergruppe Γ gehörige Funktion χ. Dann hängt χ von einer Gleichung des Grades $\nu=\frac{r}{r'}$ ab, deren Wurzeln sämtlich durch eine einzige unter ihnen rational ausdrückbar sind, denn $\chi_1, \chi_2, \dots \chi_\nu$ gehören sämtlich zu derselben Gruppe Γ (§ 101 Lehrsatz IX). Die Gruppe von 12) wird dadurch zu einer Gruppe Ω gemacht, denn die Gruppe von 12) ist transitiv, weil $g(z)$ irreduktibel ist. Wir erhalten somit:

Lehrsatz X. Ist G, die Gruppe der Gleichung $f(x)=0$ von der Ordnung r; besitzt G eine ausgezeichnete Untergruppe Γ

der Ordnung r'; ist ferner χ_1 eine zu Γ gehörige Funktion der Wurzeln $x_1, x_2, \ldots x_n$ von $f(x)=0$, so kann man eine irreduktible Gleichung

$$h(\chi)=\chi^\nu - A_1\chi^{\nu-1} + A_2\chi^{\nu-2} - \ldots = 0$$

vom Grade $\nu=\frac{r}{r'}$ aufstellen, deren Wurzeln sämtlich rationale Funktionen einer einzigen unter ihnen sind, und welche so beschaffen ist, dass die Adjungierung einer ihrer Wurzeln zu $f(x)=0$ die Gruppe G auf Γ reduziert.

§ 227. Lehrsatz XI. Ist Γ eine ausgezeichnete Maximaluntergruppe von G, so ist die Gruppe von $h(\chi)=0$ eine transitive, einfache Gruppe; und umgekehrt: ist Γ keine umfassendste ausgezeichnete Untergruppe von G, dann ist die Gruppe von $h(\chi)=0$ zusammengesetzt.

Wir bezeichnen die Gruppe von $h(\chi)=0$ durch G'; ihre Ordnung ist $\nu=\frac{r}{r'}$. Wir nehmen an, G' besitze eine ausgezeichnete Untergruppe Γ', deren Ordnung r' sein möge. Nach dem Lehrsatze IX) ist G' zu G r'-stufig isomorph. Aus den auf S. 98 § 88 abgeleiteten Sätzen folgt, dass diejenige Untergruppe J von G, welche der Gruppe Γ' entspricht, eine ausgezeichnete Untergruppe von G sein und dass sie die Ordnung $\nu'.r'$ haben wird. J ist also wie Γ ausgezeichnete Untergruppe von G; die Ordnungen beider sind $\nu'.r'$, respektive r'. Wir zeigen, dass Γ in J enthalten ist. Dies folgt einfach aus der Bildung von G' (§ 226), der zufolge die Substitution 1 von G' allen den Substitutionen von G entspricht, welche die Reihe 11) unangetastet lassen: Γ in G entspricht also der einen Substitution 1 in G'. Daher ist J umfassender als Γ; denn es entspricht der Gruppe Γ' in G'. Ist also G' zusammengesetzt, so ist Γ nicht ausgezeichnete Maximaluntergruppe von G.

In gleicher Weise wird durch Eigenschaften isomorpher Gruppen die Umkehrung des Satzes bewiesen.

§ 228. Wir beachten weiter, dass mit jeder Reduktion der Gruppe eine Zerfällung der Galois'schen Resolventengleichung Hand in Hand geht (Lehrsatz IV), während eine Zerfällung der Gleichung $f(x)=0$ nicht einzutreten braucht.

Hiernach gelangen wir zu folgendem zusammenfassenden Theoreme:

Lehrsatz XII. Ist die Gruppe G einer Gleichung $f(x)=0$ zusammengesetzt, und ist

$$G,\ G_1,\ G_2,\ \ldots\ G_\nu,\ 1$$

eine zu G gehörige Reihe der Zusammensetzung, so dass jede der Gruppen $G_1,\ G_2,\ \ldots\ G_\nu,\ 1$ eine ausgezeichnete Maximaluntergruppe der vorhergehenden Gruppe der Reihe ist; sind ferner die Ordnungen der einzelnen Gruppen

$$r,\ r_1,\ r_2,\ \ldots\ r_\nu,\ 1,$$

so kann man das Problem der Auflösung von $f(x)=0$ in folgender Weise reduzieren: Man hat der Reihe nach je eine Gleichung des Grades

$$\frac{r}{r_1},\ \frac{r_1}{r_2},\ \frac{r_2}{r_3},\ \ldots\ \frac{r_{\nu-1}}{r_\nu},\ r_\nu$$

zu lösen, deren Koefficienten in dem durch die Lösung der vorhergehenden bestimmten Rationalitätsgebiete rational sind. Diese Gleichungen sind irreduktibel, einfach und so beschaffen, dass alle Wurzeln einer jeden Gleichung durch eine beliebige Wurzel derselben rational darstellbar sind. Die Ordnungen der Gruppen dieser Gleichungen sind respektive

$$\frac{r}{r_1},\ \frac{r_1}{r_2},\ \frac{r_2}{r_3},\ \ldots\ \frac{r_{\nu-1}}{r_\nu},\ r_\nu.$$

Hierbei wird die Galois'sche Resolventengleichung, welche ursprünglich irreduktibel und vom Grade r war, der Reihe nach in

$$\frac{r}{r_1},\ \frac{r}{r_2},\ \frac{r}{r_3},\ \ldots\ \frac{r}{r_\nu},\ r$$

Faktoren zerlegt. Nach der letzten Operation ist also $f(x)=0$ vollkommen gelöst.

§ 229. Die Zusammensetzung der Gruppe G einer Gleichung $f(x)=0$ äussert sich, wie wir sehen, bei der Zerfällung der Galois'schen Resolventengleichung. Wir verweilen für einen Augenblick bei der Frage, wann eine Zerfällung des vorgelegten Gleichungspolynoms $f(x)$ selbst eintritt? Es ist leicht ersichtlich, dass beim Übergange von G_α zu $G_{\alpha+1}$ in der Reihe der Zusammensetzung von G dann und nur dann eine Zerlegung eintreten wird, wenn $G_{\alpha+1}$ nicht mehr alle die Elemente transitiv verbindet, welche durch G_α transitiv verbunden sind. § 79, S. 86 klärt uns über die hierbei eintretenden Verhältnisse auf: G_α ist imprimitiv in Hinsicht auf die transitiv verbundenen Elemente, welche bei $G_{\alpha+1}$ intransitiv auseinander treten.

Gehen wir von G aus, so ist $f(x)=0$ irreduktibel; so bleibe es beim Fortschreiten zu $G_1,\ G_2,\ \ldots\ G_\alpha$ bis für $G_{\alpha+1}$ Intransitivität, also

nach § 79 für G_α Imprimitivität eintritt. Dann zerfällt $f(x)$ in so viele Faktoren, als intransitive Systeme von Elementen hervorgerufen werden. Es treten (wieder nach § 79) in $G_{\alpha+1}$ gleichfalls alle Elemente auf. Wir ordnen jetzt die Substitutionen von G_α in eine Tabelle ein, wobei wir die Systeme der Intransitivität von $G_{\alpha+1}$ berücksichtigen. Es mögen μ solcher Systeme bestehen, so dass $f(x)$ in μ Faktoren zerlegt wird. Dann schreiben wir in die erste Zeile der Tabelle alle und nur diejenigen Substitutionen von G_α, welche die Elemente des ersten Systems der Intransitivität nicht in Elemente anderer Systeme überführen. Die Substitutionen dieser Zeile bilden eine Gruppe, welche $G_{\alpha+1}$ als Untergruppe enthält; ihre Ordnung ist demnach $\varkappa . r_{\alpha+1}$. Die zweite Zeile enthalte alle die Substitutionen von G_α, welche auf das erste das zweite System der Intransitivität folgen lassen; ihre Anzahl ist gleichfalls $\varkappa . r_{\alpha+1}$. Solcher Zeilen giebt es μ; in ihnen stehen alle Substitutionen von G_α; folglich ist

$$\mu . \varkappa . r_{\alpha+1} = r_\alpha; \quad \mu = \frac{1}{\varkappa} \frac{r}{r_{\alpha+1}},$$

d. h. die Anzahl der Faktoren μ, in welche $f(x)$ zerfällt, ist ein Teiler der Anzahl $\frac{r_\alpha}{r_{\alpha+1}}$ der Faktoren, in welche gleichzeitig die Galois'sche Resolventengleichung zerfällt. Das entsprechende geschieht offenbar bei jeder späteren Zerfällung.

---

§ 230. Bisher haben wir der gegebenen Gleichung $f(x) = 0$ alle Wurzeln einer anderen Gleichung $g(\psi) = 0$ oder $h(\chi) = 0$ adjungiert, deren Wurzeln rationale Funktionen von $x_1, x_2, \ldots$ waren. Dies scheint eine starke Einschränkung zu sein. Wir wollen daher jetzt der Gleichung $f(x) = 0$ alle Wurzeln einer irreduktiblen Gleichung

$$13) \qquad k(z) = 0$$

adjungieren, von der wir nur wissen, dass sich ihre Koefficienten im Rationalitätsbereiche von $f(x) = 0$ befinden. Wir nehmen an, dass durch die Adjungierung die Gruppe G der Gleichung $f(x) = 0$ reduziert, die Resolventengleichung also in Faktoren zerlegt werde. Hieraus suchen wir über die Natur von 13) ins klare zu kommen.

Dieselbe Gruppenreduktion, wie sie durch Adjungierung der Wurzeln von 13) erreicht wird, können wir durch die Adjungierung einer rationalen Funktion $\psi_1(x_1, x_2, \ldots x_n)$ der Wurzeln von $f(x) = 0$ erreichen. Denn reduziert sich G auf H, so braucht man nur ψ als zur Gattung von H gehörig anzunehmen. ψ_1 ist demnach nach der Lösung von 13) rational bekannt, so dass wir setzen können

$$\psi_1(x_1, x_2, \ldots x_n) = \Psi_1(z_1, z_2, \ldots z_m) = u_1.$$

Die Gleichung, welche ψ_1 liefert, ist somit identisch mit derjenigen, welche Ψ_1 liefert. Sie sei

$$14) \qquad l(u) = 0.$$

Alle Werte, welche ψ_1 im Rationalitätsbereiche annehmen kann, werden durch die Wurzeln von 14) geliefert; alle diese sind aber gleichzeitig Werte von Ψ_1, d. h. sie werden nach der Lösung von 13) bekannt. Also sind die Werte von ψ_1, welche als Wurzeln von 14) auftreten, sämtlich der Gleichung $f(x) = 0$ zu adjungieren. H ist daher eine ausgezeichnete Untergruppe von G.

Lehrsatz XIII. Die Einwirkung, welche die Adjungierung aller Wurzeln einer beliebigen Gleichung 13) auf die Reduktion der Gruppe G von $f(x) = 0$ ausübt, kann durch diejenige aller Wurzeln einer Gleichung 14) ersetzt werden, welche durch rationale Funktionen $x_1, x_2, \ldots x_n$ befriedigt wird.

Wir befinden uns also, trotz unserer Loslösung von scheinbaren Beschränkungen, durchaus innerhalb der früher besprochenen Verhältnisse, bei denen zur Adjungierung nur rationale Funktionen der Wurzeln zugelassen wurden.

§ 231. Hiernach lässt sich umgekehrt auch die Einwirkung bestimmen, welche die Lösung von $f(x) = 0$ auf $k(z) = 0$ hat, falls durch die Lösung von $k(z) = 0$ eine Reduktion bei $f(x) = 0$ eintritt. Durch die Lösung von $f(x) = 0$ wird ψ_1 bekannt, damit auch Ψ_1, und 14) ist gelöst. Denn 14) ist so beschaffen, dass die Adjungierung aller Wurzeln dieselbe Gruppe H hervorruft, wie die Adjungierung einer einzigen Wurzel ψ_1 zu $f(x) = 0$, und folglich sind alle Wurzeln von (14) rational durch ψ_1 darstellbar. Dasselbe gilt, wenn man die $\Psi_1(z_1, z_2 \ldots)$ als Wurzeln ansieht, so dass $\Psi_1, \Psi_2, \ldots$ zu derselben Gruppe der Elemente z gehören, und dass diese Gruppe der Ordnung ν eine ausgezeichnete Untergruppe der Gruppe von $k(z)$ ist.

Lehrsatz XIV. Sind

$$f(x) = 0, \quad k(z) = 0$$

zwei Gleichungen, deren Koefficienten demselben Rationalitätsbereiche angehören und welche so beschaffen sind, dass durch die Lösung der zweiten und die Adjungierung aller ihrer Wurzeln zur ersteren die Gruppe von $f(x) = 0$ auf eine in ihr enthaltene ausgezeichnete Untergruppe von ν mal geringerer Ordnung reduziert wird, so wird auch umgekehrt

durch die Lösung der ersten die Gruppe der zweiten auf den ν^{ten} Teil ihrer Substitutionen reduziert. Die Gruppe von $f(x)=0$, wie die von $k(z)=0$, ist zusammengesetzt, und ν ist ein Zahlenfaktor der Komposition. Diejenigen rationalen Funktionen einer der beiden Gleichungen, durch welche die Reduktion ihrer Gruppe in derselben Art bewirkt werden kann, wie durch die Lösung der anderen Gleichung, sind rational durch die Wurzeln derselben darstellbar.

Es kann, wie man sieht, die Gruppe von $f(x)=0$ auch durch die Auflösung einer Gleichung $k(z)=0$ reduziert werden, trotzdem die Wurzeln derselben keine rationale Funktionen von $x_1, x_2, \ldots x_n$ sind; es muss eben nur rationale Funktionen von $z_1, z_2, \ldots z_m$ geben, welche rationalen Funktionen von $x_1, x_2, \ldots x_n$ gleich sind.

Aus dem vorigen Lehrsatze folgen unmittelbar die Corollare:

Zusatz I. Wenn die Gruppe G der Gleichung $f(x)=0$ einfach ist, kann sie nur mit Hilfe von Gleichungen aufgelöst werden, bei denen die Ordnung der Gruppen Vielfache der Ordnung von G sind.

Denn da G auf 1 reduziert wird, so ist das ν im Lehrsatz XIV) gleich der Ordnung von G zu setzen.

Zusatz II. Wenn die Gruppe G von $f(x)=0$ durch die Auflösung einer einfachen Gleichung $k(z)=0$ reduziert wird, dann sind $z_1, z_2, \ldots z_m$ rationale Funktionen der Wurzeln von $f(x)=0$.

Denn in diesem Falle ist ν gleich der Ordnung der Gruppe von $k(z)=0$; diese wird nach der Reduktion gleich 1, also ist

$$\Psi_1 = \alpha_1 z_1 + \alpha_2 z_2 + \ldots + \alpha_m z_m = \psi_1(x_1, x_2, \ldots x_n)$$

zu setzen; Ψ_1 ist die Galois'sche Resolvente von $k(z)=0$.

§ 232. Ebensowenig wie durch die Adjungierung der Wurzeln einer neuen Gleichung $k(z)=0$ zu $f(x)=0$ eine Erweiterung gegenüber der Adjungierung rationaler Funktionen der Gleichungswurzeln selbst erzielt werden kann, ebensowenig findet dies statt, wenn die Wurzeln beider Gleichungen in einen und denselben rationalen Ausdruck eingehen. Wir werden beweisen:

Lehrsatz XV. Sind

$$f(x)=0, \quad k(z)=0$$

zwei irreduktible Gleichungen, deren Wurzeln durch rationale Beziehungen

$$\varphi(x_1, x_2, \ldots x_n;\ z_1, z_2, \ldots z_m) = 0$$

mit einander zusammenhängen, so können alle diese aus einer einzigen von der Form

$$\psi(x_1, x_2, \ldots x_n) = \chi(z_1, z_2, \ldots z_m)$$

abgeleitet werden, in welcher die Wurzeln beider Gleichungen getrennt auftreten.

Bezeichnen wir nämlich mit ξ, ζ die bezüglichen Galois'schen Resolventen und mit

$$F(\xi) = 0, \quad K(\zeta) = 0$$

die irreduktiblen Resolventengleichungen, welche zu $f(x) = 0$, $k(z) = 0$ gehören, so werden die Grade r, r' von F, K gleich den Ordnungen der Gruppen sein.

Jetzt kann man $x_1, x_2, \ldots x_n$ rational durch ξ und $z_1, z_2, \ldots z_m$ rational durch ζ ausdrücken und erhält dadurch

$$\varphi(x_1, x_2, \ldots x_n;\ z_1, z_2, \ldots z_m) = \Phi(\xi, \zeta) = 0.$$

Der Ausdruck Φ kann mit Hilfe von $F = 0$ und $K = 0$ so reduziert werden, dass sein Grad in ξ höchstens gleich $r - 1$, in ζ höchstens gleich $r' - 1$ wird. Wir setzen dies als geschehen voraus. Dann haben die Gleichungen

$$\Phi(\xi, \zeta) = 0, \quad F(\xi) = 0$$

eine Wurzel gemeinsam. Folglich kann, wenn man ζ zum Rationalitätsbereiche zieht, die Resolvente $F(\xi)$ nicht mehr irreduktibel sein, weil sonst die irreduktible Gleichung r^{ten} Grades mit einer Gleichung, die höchstens bis zum $r - 1^{\text{ten}}$ Grade aufsteigt, eine Wurzel gemeinsam hätte; ausgenommen ist dabei der Fall, dass $\Phi(\xi, \zeta)$ identisch Null wird.

Tritt dies nicht ein, so wird durch die Adjungierung aller Wurzeln von $k(z) = 0$ oder durch die von ζ, die Resolvente von $f(x) = 0$ zerlegt; also befinden wir uns in der Lage der vorigen Paragraphen; durch Adjungierung einer Funktion χ von $x_1, x_2, \ldots x_n$ können wir dieselbe Reduktion erreichen und es wird

$$\chi(x_1, \ldots x_n) = \psi(z_1, z_2, \ldots z_m).$$

Existieren mehrere derartige Beziehungen, so können alle aus derselben Gleichung abgeleitet werden. Diese lässt sich leicht finden, wenn man eine Funktion χ so wählt, dass alle anderen unter der ihr angehörenden Gattung enthalten sind.

Wenn dagegen $\Phi(\xi, \zeta) = 0$ identisch gleich Null ist, so folgt daraus, dass die Koefficienten des nach ξ geordneten Polynoms $\Phi(\xi, \zeta)$, d. h. Funktionen von der Form $\chi_1(\zeta)$ oder

$$\chi_2(z_1, z_2, \ldots z_m) = 0$$

sind. Ebenso müssen dann auch Funktionen von der Form $\psi_1(\xi)$ oder

$$\psi_2(x_1, x_2, \ldots x_n) = 0$$

werden, wenn man $\Phi(\xi, \zeta)$ nach Potenzen von ζ anordnet.

Diese Gleichungen können in der That $\varphi = 0$ machen; dadurch wird aber nur eine scheinbare, keine wirkliche Abhängigkeit der Wurzeln von $f(x) = 0$, $k(z) = 0$ konstituiert; $\chi_2 = 0$ wird zur Gruppe von $k(z) = 0$, $\psi_2(x_1, \ldots) = 0$ zur Gruppe von $f(x) = 0$ gehören.

Fünfzehntes Kapitel.

Algebraisch auflösbare Gleichungen.

§ 233. Wir haben in § 228 folgendes Theorem aufgestellt: Wenn die Gruppe G der Gleichung $f(x) = 0$ folgende Reihe der Zusammensetzung liefert:

1) $$G, G_1, G_2, \ldots G_\nu, 1$$

und die Ordnungen der einzelnen Gruppen bezüglich

$$r, r_1, r_2, \ldots r_\nu, 1$$

sind, so kann man die Auflösung von $f(x) = 0$ durch diejenige einer Reihe von einfachen, irreduktiblen Gleichungen der Grade

$$\frac{r}{r_1}, \frac{r_1}{r_2}, \frac{r_2}{r_3}, \ldots \frac{r_{\nu-1}}{r_\nu}, r_\nu$$

bewirken, deren erste eine zur Gattung G_1 gehörige Funktion liefert, während die Koefficienten der Gattung G angehören, deren zweite eine zur Gattung G_2 gehörige Funktion liefert, während ihre Koefficienten der Gattung G_1 angehören u. s. w. Alle diese Gleichungen

$$\chi_1 = 0, \quad \chi_2 = 0, \ldots \chi_\nu = 0, \quad \chi_{\nu+1} = 0$$

haben die Eigenschaft, dass die Wurzeln einer jeden durch eine beliebige unter denselben rational dargestellt werden können, so dass die Ordnung ihrer Gruppe dem Grade derselben gleich, d. h. dass die Gruppe vom Typus Ω (§ 122) wird.

Wir wollen untersuchen, wann alle diese Gleichungen $\chi = 0$ binomische Gleichungen von der Primzahlordnung p_λ werden und also die Form

$$\chi_\lambda \equiv z^{p_\lambda} - H_\lambda = 0$$

annehmen, wobei H_λ in den zur Gattung $G_{\lambda-1}$ gehörigen Grössen rational ist. Mit anderen Worten: wir wollen die notwendigen und hinreichenden Bedingungen dafür aufsuchen, dass $f(x)=0$ algebraisch lösbar ist.

Notwendig ist es für die Erfüllung der aufgestellten Forderungen, dass die Faktoren der Zusammensetzung $\frac{r}{r_1}, \frac{r_1}{r_2}, \frac{r_2}{r_3}, \cdots$ sämtlich Primzahlen $p_1, p_2, p_3, \ldots$ seien; denn diese Quotienten geben die Grade der Gleichungen $\chi_1=0$, $\chi_2=0$, $\chi_3=0, \ldots$ an.

Hinreichend ist dies gleichfalls. Dies wurde bereits in §§ 102 und 103, Lehrsatz X) und XII) dargethan. Nicht etwa, dass jede zu G_λ gehörige Funktion, in die p_λ^{te} Potenz erhoben, eine zu $G_{\lambda-1}$ gehörige Funktion giebt, sondern es lässt sich eine Funktion finden, für welche dies der Fall ist, sobald jene Bedingung erfüllt ist.

Wir haben daher den Satz:

Lehrsatz I. Damit die algebraische Gleichung $f(x)=0$ durch Wurzelausziehungen auflösbar sei, ist es notwendig und hinreichend, dass die Faktoren der Zusammensetzung ihrer Gruppe sämtlich Primzahlen sind.

§ 234. Mit Hilfe von Lehrsatz XIII), § 103 können wir dem soeben erhaltenen Satz eine andere Ausdrucksform geben:

Lehrsatz II. Damit die algebraische Gleichung $f(x)=0$ durch Wurzelbeziehungen auflösbar sei, ist es notwendig und hinreichend, dass man ihre Gruppe durch eine Reihe von Substitutionen

$$1, t_1, t_2, t_3, \ldots t_\nu, t_{\nu+1}$$

herstellen könne, welche folgende beiden Eigenschaften besitzen: 1) die Substitutionen der Gruppe $G_\lambda = \{1, t_1, t_2, \ldots t_{\lambda-1}, t_\lambda\}$ sind untereinander bis auf Substitutionen der Gruppe $G_{\lambda-1} = \{1, t_1, t_2, \ldots t_{\lambda-1}\}$ vertauschbar; 2) die niedrigste Potenz von t_λ, welche in $G_{\lambda-1}$ vorkommt, hat zum Exponenten eine Primzahl (vergl. auch § 83, Lehrsatz XIX).

§ 235. Ferner ermöglichen es die Untersuchungen von § 85, den ersten Lehrsatz in einer neuen, dritten Form auszusprechen. Wir sahen nämlich dort: Stimmt die zu G gehörige Hauptreihe

$$2) \qquad G, H, J, K, \ldots 1$$

nicht mit der Reihe der Zusammensetzung überein, so kann aus jener ersteren 2) die letztere 1) durch Einschiebung neuer Gruppen, z. B. von

3) $$H', H'', \ldots H^{(\lambda)}$$

zwischen H und J u. s. f. abgeleitet werden. Dann sind die Faktoren der Zusammensetzung, welche zum Übergange von H zu H', von H' zu H'', ... von $H^{(\lambda)}$ zu J gehören, einander sämtlich gleich. Sind demnach nicht alle zu 1) gehörigen Faktoren der Zusammensetzung einander gleich, so hat G eine Hauptreihe der Zusammensetzung 2). Wir sahen ferner (§ 86 S. 96): stets wenn die zum Übergange von H, H', H'', ... zur jedesmalig folgenden Gruppe gehörigen Faktoren der Zusammensetzung Primzahlen sind (die einander nach dem soeben Besprochenen natürlich gleich werden), und nur, wenn dies der Fall ist, sind die Substitutionen von H untereinander bis auf Substitutionen von J vertauschbar. Daraus folgt:

Lehrsatz III. Damit die algebraische Gleichung $f(x)=0$ durch Wurzelausziehungen auflösbar sei, ist es notwendig und hinreichend, dass ihre Hauptreihe der Zusammensetzung

2) $$G, H, J, K, \ldots 1$$

folgende Eigenschaft besitze: die Substitutionen jeder Gruppe sind bis auf Substitutionen der nächstfolgenden Gruppe mit einander vertauschbar.

Die Substitutionen der letzten Gruppe der Hauptreihe, welche der Einheit vorhergeht, sind daher untereinander vertauschbar.

§ 236. Bevor wir in der Theorie weiter gehen, wollen wir einige Anwendungen der bisher abgeleiteten Sätze geben:

Lehrsatz IV. Ist eine Gruppe Γ einstufig isomorph zu einer auflösbaren Gruppe G, so ist auch Γ eine auflösbare Gruppe.

Nach S. 98 stimmen die Faktoren der Zusammensetzung von G mit denen von Γ überein. Daher folgt unser jetziges Theorem unmittelbar aus dem ersten Lehrsatz.

Lehrsatz V. Ist eine Gruppe Γ mehrstufig isomorph zu der auflösbaren Gruppe G; entspricht ferner der Substitution 1 von G die Untergruppe Σ von Γ; ist endlich auch Σ eine auflösbare Gruppe, so wird Γ gleichfalls auflösbar sein.

Die Faktoren der Zusammensetzung von Γ bestehen nach S. 98 aus denen von G und denen von Σ. Die Anwendung von Lehrsatz I) zeigt demnach die Richtigkeit unseres Theorems.

Lehrsatz VI. Ist eine Gruppe G auflösbar, so sind es auch alle ihre Untergruppen.

Wir setzen wie gewöhnlich

$$\xi_1 = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n,$$

wenden auf ξ_1 die Substitutionen von G an, erhalten $\xi_1, \xi_2, \ldots \xi_r$ und bilden

$$g(\xi) \equiv (\xi - \xi_1)(\xi - \xi_2)\ldots(\xi - \xi_r) = 0.$$

Es ist charakteristisch für die Auflösbarkeit von G und dass man mit Hilfe von Wurzelausziehungen $g(\xi)$ in lineare Faktoren zerlegen kann.

Ist nun H von der Ordnung r_1 eine Untergruppe von G und liefert diese bei ihrer Anwendung auf ξ_1 die Werte $\xi_1, \xi_2, \ldots \xi_{r_1}$, so sind diese sämtlich unter $\xi_1, \xi_2, \ldots \xi_r$ enthalten; folglich ist

$$h(\xi) \equiv (\xi - \xi_1)(\xi - \xi_2)\ldots(\xi - \xi_{r_1})$$

ein Teiler von $g(\xi)$. Daher lässt sich auch $h(\xi)$ mit Hilfe von Wurzelausziehungen in lineare Faktoren zerlegen, d. h. es ist H eine auflösbare Gruppe.

Man hätte den Beweis auch dadurch führen können, dass man zeigt, alle Faktoren der Zusammensetzung von H kämen unter denen von G vor.

Lehrsatz VII. Ist die Ordnung einer Gruppe G die Potenz einer Primzahl p, so ist die Gruppe eine auflösbare.

Die Gruppe G ist von gleichem Typus mit einer Untergruppe derjenigen, welche denselben Grad n besitzt wie G und als Ordnung die höchste Potenz p^f, welche $n!$ teilt (vergl. §§ 49 und 39). Dass diese letztere aber auflösbar ist, folgt aus ihrer Bildung (§ 39), bei welcher sich herausstellt, dass alle ihre Faktoren der Zusammensetzung gleich der Primzahl p werden. Nach dem vorigen Satze ist also auch G auflösbar.

Lehrsatz VIII. Ist die Ordnung einer Gruppe G einer algebraischen Gleichung $f(x) = 0$

$$r = p_1^{\alpha} \cdot p_2^{\beta} \cdot p_3^{\gamma} \cdot p_4^{\delta} \ldots,$$

wobei $p_1, p_2, p_3, \ldots$ von einander verschiedene Primzahlen sind, und

$$p_1 > p_2^{\beta} \cdot p_3^{\gamma} \cdot p_4^{\delta} \ldots, \quad p_2 > p_3^{\gamma} \cdot p_4^{\delta} \ldots, \quad p_3 > p_4^{\delta} \ldots$$

ist, dann ist die Gleichung durch Wurzeln auflösbar.*

Wir benutzen das Theorem von S. 132, § 121. Wir setzen $r = p_1^{\alpha} \cdot q$, wo dann $p_1 > q$ wird. G enthält mindestens eine Untergruppe H der

* L. Sylow: Math. Ann. V, S. 589.

Ordnung p_1^{α}; bezeichnen wir durch $(\varkappa p_1 + 1)$ die Anzahl aller in G enthaltenen Untergruppen der Ordnung p_1^{α}, und durch $p_1^{\alpha}.i$ die Ordnung der Maximaluntergruppe von G, welche mit H vertauschbar ist, so wird $r = p_1^{\alpha}.i(\varkappa p_1 + 1)$. Da $r = p_1^{\alpha}.q$ und $q < p_1$ ist, so muss $\varkappa = 0$ und $r = p_1^{\alpha}.i$ gesetzt werden, d. h. G selbst ist mit H vertauschbar. Durch die Lösung einer Hilfsgleichung des Grades q, deren Gruppe die Ordnung q besitzt, kommt man daher zu einer Funktion, welche der Gattung H angehört, und die Gruppe G reduziert sich auf H (§ 226, Lehrsatz X). Die letztere Gruppe ist nach dem vorigen Lehrsatze lösbar. Wenn also die Hilfsgleichung lösbar ist, so ist es auch $f(x) = 0$ selbst.

Die Ordnung der Hilfsgleichung $q = p_2^{\beta}.p_3^{\gamma}.p_4^{\delta}\ldots$ giebt zu denselben Schlüssen Veranlassung, da dieselben Voraussetzungen gelten wie vorher. Ihre Auflösbarkeit folgt deswegen aus der einer neuen Hilfsgleichung mit einer Gruppe der Ordnung $p_3^{\gamma}.p_4^{\delta}\ldots$ u. s. w.

§ 237. Wir kehren zu den allgemeinen Untersuchungen von § 235 zurück.

Beim Übergange von G zu G_1 zerfällt die Galois'sche Resolventengleichung in $\frac{r}{r_1} = p_1$ Faktoren; beim Übergange von G_1 zu G_2 zerfällt jeder dieser vorher irreduktiblen Faktoren in $\frac{r_1}{r_2} = p_2$ neue Faktoren u. s. w.

Da $f(x)$ anfangs irreduktibel, schliesslich aber in lineare Faktoren zerlegt ist, so wird nach § 229 ein oder mehrere Male eine Zerfällung von $f(x)$ oder von einem seiner bereits vorhandenen rational bekannten Faktoren zugleich mit der Zerfällung der Galois'schen Resolventengleichung oder deren bereits rational bekannten Faktoren eintreten. Die Anzahl der Faktoren bei der Zerfällung von $f(x)$, welche natürlich grösser als 1 wird, muss nach § 229 ein Teiler der Anzahl der Faktoren sein, welche bei der Zerfällung der Resolventengleichung auftreten. Diese letztere Anzahl ist bei auflösbaren Gleichungen stets eine Primzahl $p_1, p_2, p_3, \ldots$; also findet dasselbe bei $f(x) = 0$ statt. Das heisst: Alle Primfaktoren des Grades n der auflösbaren Gleichung $f(x) = 0$ sind Faktoren der Zusammensetzung der Gruppe G und zwar jeder mindestens so oft, als er in n als Faktor vorkommt.*

* Um einem naheliegenden Irrtume vorzubeugen, sei erwähnt, dass, wenn beim Vordringen von G aus bis zu G_λ das Polynom $f(x)$ in rationale Faktoren zerfällt, deren einer $f_\lambda'(x)$ ist, dieser Faktor nicht zur Gruppe G_λ zu gehören braucht.

Wir wollen nun annehmen, dass n nicht die Potenz einer Primzahl sei, dass n also von einander verschiedene Primzahlen zu Faktoren hat. Dann kommen auch unter den Faktoren der Zusammensetzung der Reihe von G verschiedene Primzahlen vor, und daher besitzt G nach § 85 Zusatz I) eine Hauptreihe. Diese sei

2) $$G, H, J, K, \ldots M, 1.$$

In einer der zu G gehörigen Reihen der Zusammensetzung mögen zwischen H und J noch

3) $$H', H'', \ldots H^{(\lambda)}$$

aufzunehmen sein. Da n mindestens zwei von einander verschiedene Primzahlen zu Faktoren hat, so muss $f(x)$ mindestens zwei mal beim Übergange von einer Gruppe der Reihe der Zusammensetzung zur folgenden in Faktoren zerfallen. Da die Anzahl der Faktoren mit dem Faktor der Zusammensetzung übereinstimmt, und da dieser bei den Zwischengruppen 3) sich nicht ändert, so können nicht beide Zerfällungen innerhalb desselben Überganges von einem Gliede H der Hauptreihe zum nächstfolgenden Gliede J derselben eintreten. Besonders hervorzuheben ist, dass nicht alle Zerfällungen von $f(x)$ innerhalb des Überganges von der letzten Gruppe M bis zu 1, also innerhalb der auf M folgenden Gruppen der Reihe der Zusammensetzung

$$M', M'', M''', \ldots M^{(\varkappa-1)}, 1$$

stattfinden können. Mindestens eine der Zerfällungen muss sich früher vollzogen haben. Die erste derselben finde z. B. statt beim Übergange von H' zu H''. Dann folgt aus § 229, dass H' imprimitiv ist in denjenigen Elementen, welche sie transitiv verbindet, und dass H'' diese transitiv verbundenen Elemente in einzelne Systeme der Intransitivität zerteilt hat und nur diejenigen weiterhin mit einander transitiv verbinden kann, welche demselben System der Imprimitivität von H' angehören. Diese Intransitivität pflanzt sich dann auf alle späteren enthaltenen Gruppen $H''', \ldots H^{(\nu)}$ und ebenso auf das nächste Glied J der Hauptreihe fort, welches der Voraussetzung zufolge von 1 verschieden ist.

J möge die Wurzeln in die intransitiven Systeme

$$x_1', x_2', \ldots x_i'; \quad x_1'', x_2', \ldots x_i''; \ldots; \quad x_1^{(m)}, x_2^{(m)}, \ldots x_i^{(m)}$$

Er kann auch unter der zu G_λ gehörigen Gattung stehen. Die Anzahl der Werte von $f_\lambda'(x)$ ist folglich nicht notwendig gleich $\frac{r}{r_\lambda}$; sie kann auch ein Vielfaches dieses Quotienten sein; und das Produkt $f_\lambda'(x) . f_\lambda''(x) \ldots$ aller Werte von $f_\lambda'(x)$ ist nicht notwendig gleich $f(x)$; es kann auch eine Potenz dieses Polynoms sein.

zerlegen; diese mögen so wenig umfangreich als möglich gewählt sein. Dann wird jetzt der Ausdruck

$$f_\lambda'(x) = (x - x_1')(x - x_2') \ldots (x - x_i')$$

ein rational bekannter Faktor von $f(x)$ sein, welcher keine rational bekannten Teiler mehr enthält. Da wegen der Eigenschaften der Gruppen der Hauptreihe

$$G^{-1}JG = J$$

ist, so gehören alle Werte von $f_\lambda'(x)$ zu derselben Gruppe J; sie sind also mit $f_\lambda'(x)$ gleichzeitig bekannt. Ausser $f_\lambda'(x)$ kennen wir noch als Werte dieses Ausdrucks

$$\begin{aligned}
f_\lambda''(x) &= (x - x_1'')\ (x - x_2'')\ \ldots (x - x_i''),\\
f_\lambda'''(x) &= (x - x_1''')\ (x - x_2''')\ \ldots (x - x_i'''),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
f_\lambda^{(m)}(x) &= (x - x_1^{(m)})\ (x - x_2^{(m)}) \ldots (x - x_i^{(m)}).
\end{aligned}$$

Existierte ausser diesen noch ein neuer, so würde derselbe mit einem $f_\lambda^{(\alpha)}(x)$ Wurzeln gemeinsam haben. Somit liesse sich $f_\lambda^{(\alpha)}(x)$ und also noch $f_\lambda'(x)$ in rationale Faktoren zerlegen, was den Annahmen widerspricht. Folglich hat $f_\lambda'(x)$ auch nur $m = \frac{n}{i}$ Werte und hängt somit von der Lösung einer Gleichung des Grades m ab. Ist diese Gleichung m^{ten} Grades

$$4) \qquad \varphi(y) \equiv (y - f_\lambda')(y - f_\lambda'') \ldots (y - f_\lambda^{(m)}) = 0,$$

so entsteht $f(x)$ durch Elimination von y aus 4) und aus

$$5) \qquad f_\lambda'(x) \equiv x^i - \psi_1(y')x^{i-1} + \psi_2(y')x^{i-2} - \ldots = 0,$$

wobei

$$\begin{aligned}
\psi_1(y') &= x_1' + x_2' + x_3' + \ldots + x_i',\\
\psi_2(y') &= x_1'x_2' + x_1'x_3' + x_2'x_3' + \ldots + x_{i-1}'x_i',\\
&\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

ist, so dass $\psi_1, \psi_2, \ldots$ rational durch f_λ' ausdrückbar sind. Da $f(x)$ das Eliminationsresultat von 4) und 5) ist, so wird nach § 222 die Gruppe von $f(x)$ imprimitiv sein.

Das ganze Gewicht der durchgeführten Schlüsse beruht auf dem Umstande, dass J der Hauptreihe von G angehört, und dass also $G^{-1}JG = J$ ist. Nur daraus war der Schluss zu ziehen, dass alle im Rationalitätsgebiete von $f(x)$ vorhandenen Werte von $f_\lambda'(x)$ bekannt sind. Es wird sich dies besonders deutlich an einem sofort zu behandelnden Beispiele herausstellen.

Lehrsatz IX. Ist der Grad n einer algebraischen, irreduktiblen, auflösbaren Gleichung durch zwei von einander verschiedene Primzahlen teilbar, so kann man n stets in zwei Faktoren $n = i.m$ derart zerlegen, dass die gegebene Gleichung $f(x) = 0$ in m neue zerfällt

$$f_i'(x) = 0, \quad f_i''(x) = 0, \ldots f_i^{(m)}(x) = 0,$$

welche sämtlich vom Grade i sind und deren Koefficienten aus den rational bekannten Grössen durch die Auflösung einer Gleichung des Grades m abgeleitet werden können.* Die Gruppe der Gleichung $f(x) = 0$ ist imprimitiv.

Wir wollen hiermit die Auflösung der allgemeinen Gleichung vierten Grades vergleichen, auf welche, da $4 = 2^2$ ist, die obigen Schlüsse nicht anwendbar sind. Es zeigt sich sofort, dass beide für die Zerlegung des Polynoms in lineare Faktoren notwendigen Zerfällungen erst innerhalb des Bereiches der letzten Gruppe der Hauptreihe $M, M', M''', \ldots 1$ vorkommen. Die Reihe der Gleichung besteht aus den folgenden Gruppen:

1) die symmetrische Gruppe;
2) die alternierende Gruppe;
3) $[1, (x_1x_2)(x_3x_4), (x_1x_3)(x_2x_4), (x_1x_4)(x_2x_3)]$;
4) $[1, (x_1x_2)(x_3x_4)]$; oder 4') $[1, (x_1x_3)(x_2x_4)]$;
   oder 4'') $[1, (x_1x_4)(x_2x_3)]$;
5) die Gruppe 1.

Die Hauptreihe wird aus den Gruppen 1), 2), 3), 5) gebildet. Der Übergang von 3) zu 4) und von 4) zu 5) liefert jedesmal den Primfaktor 2. Die Gruppe 4) ist die erste intransitive. Bei ihr tritt ein Zerfallen von $f(x)$ in zwei Faktoren $(x-x_1)(x-x_2)$ und $(x-x_3)(x-x_4)$ ein. Da aber 4) nicht zur Hauptreihe gehört, so sind nicht alle sechs Werte von $(x-x_1)(x-x_2)$ bekannt; hätte man die Gruppe 4') gewählt, so wäre man auf $(x-x_1)(x-x_3)$ und $(x-x_2)(x-x_4)$ gekommen u. s. f. Das Produkt dieser sechs Werte liefert die dritte Potenz von $f(x) = (x-x_1)(x-x_2)(x-x_3)(x-x_4)$. Man kann also zwar $f(x)$ in ein Produkt aus zwei Faktoren zweiten Grades zerlegen; aber die Koefficienten eines jeden solchen Produktes sind nicht von einer Gleichung des Grades $\frac{4}{2} = 2$, sondern von einer solchen des Grades 6 abhängig.

* Abel: Oeuvres complètes II, p. 191.

Betrachten wir ferner die irreduktiblen auflösbaren Gleichungen sechsten Grades, so folgt, dass es für sie zwei verschiedene Arten giebt, jenachdem man y aus

$$x^2 - f_1(y)x + f_2(y) = 0, \quad y^3 - c_1y^2 + c_2y - c_3 = 0$$

oder aus

$$x^3 - f_1(y)x^2 + f_2(y)x - f_3(y) = 0, \quad y^2 - c_1y + c_2 = 0$$

eliminiert, so dass jede auflösbare, irreduktible Gleichung sechsten Grades einer dieser beiden Arten angehört.

§ 238. Wir können nach den Resultaten unserer Untersuchungen die einschränkende Voraussetzung machen, dass der Grad der betrachteten Gleichung $f(x) = 0$ die Potenz einer Primzahl sei; denn andernfalls können wir die Gleichung als Eliminationsresultat behandeln und dadurch die Frage vereinfachen. Weiter können wir voraussetzen, dass eine derartige Zerlegung, wie sie im vorigen Lehrsatze angegeben war, bei unserer Gleichung des Grades p^λ nicht vorkomme, da sonst eine gleiche Vereinfachung möglich wäre. Dies erreichen wir durch die Annahme, dass die Gruppe der Gleichung primitiv sein soll. Dann sind beide Möglichkeiten abgeschnitten.

Unter solcher Annahme gehen wir zur Untersuchung der Gruppe über.

Der Grad der Gleichung sei p^λ; die Hauptreihe der Zusammensetzung ihrer Gruppe

$$2) \qquad G, H, J, K, \ldots M, 1.$$

Geht man von G über $H, J, \ldots$ bis M, so kann bis dorthin noch keine Zerlegung des Polynoms $f(x)$ stattgefunden haben; denn sonst könnten die Schlüsse des vorigen Paragraphen in Anwendung gebracht werden, und diese würden zeigen, dass G imprimitiv ist. Durch den Übergang von G bis zu M wird die Gleichung $f(x) = 0$ zur Auflösung „vorbereitet“, aber $f(x)$ wird noch nicht in Faktoren zerfällt. Die λ Zerfällungen der Gleichung des Grades p^λ treten demnach beim Übergang von der letzten Gruppe der Hauptreihe bis zur Einheit auf, d. h. bei

$$M, M', M'', M''', \ldots M^{(\varkappa-1)}, 1;$$

es muss demnach $\varkappa \geq \lambda$ sein. Die Anwendung von § 85 Zusatz IV) (S. 95) ergiebt, dass alle Substitutionen von M unter einander vertauschbar sind. Die durch die Gattung M charakterisierte Gleichung ist sonach eine Abel'sche Gleichung des Grades p^λ (§ 180). Nach den Schlüssen von § 85 gehört zu jedem Übergange innerhalb der letzten Reihe der Faktor p der Zusammensetzung, so dass die Ordnung von

M gleich $p^\varkappa$ zu setzen ist. Ferner kann M erhalten werden, wenn man eine Anzahl von $\varkappa$ Gruppen mit einander vereinigt, welche nur die Einheit als gemeinsame Substitution besitzen, einander ähnlich sind und p zur Ordnung haben. Es mögen dies sein:

$$M^{(\varkappa-1)},\ M_1^{(\varkappa-1)},\ M_2^{(\varkappa-1)},\ \ldots\ M_{\varkappa-1}^{(\varkappa-1)}.$$

Aus diesen Eigenschaften ist ersichtlich, dass jede dieser Gruppen aus den Potenzen einer Substitution der Ordnung p gebildet ist:

$$s,\ s_1,\ s_2,\ \ldots\ s_{\varkappa-1},$$

und dass wegen der Vertauschbarkeit der Gruppen (vergl. S. 96 oben) auch

$$s_\alpha^\mu s_\beta^\nu = s_\beta^\nu s_\alpha^\mu \quad (\alpha, \beta = 0, 1, \ldots \varkappa - 1)$$

sein muss. Jede Substitution von M kann demnach durch

$$s^\lambda s_1^\mu s_2^\nu \ldots s_{\varkappa-1}^\tau$$

ausgedrückt werden. Wegen der Vertauschbarkeit der s unter einander ist

$$(s^\lambda s_1^\mu s_2^\nu \ldots s_{\varkappa-1}^\tau)^p = s^{\lambda p} s_1^{\mu p} s_2^{\nu p} \ldots s_{\varkappa-1}^{\tau p} = 1.$$

Jede Substitution der Gruppe M ist von der Ordnung p. Unsere Abel'sche Gleichung gehört infolgedessen zur Kategorie derjenigen, welche in § 183 behandelt wurden. Ebenda (§ 184) sind auch ihre Substitutionen analytisch dargestellt worden. Es ergab sich folgende Form der Darstellung für dieselben

$$t \equiv |z_1, z_2, \ldots z_\varkappa \quad z_1 + \alpha_1,\ z_2 + \alpha_2,\ \ldots\ z_\varkappa + \alpha_\varkappa| \pmod p.$$

Schon das vollkommen gleichmässige Auftreten aller Indices $z_1, \ldots z_\varkappa$ zeigt, dass bei den Reduktionen von M bis zu 1 genau $\varkappa$ Zerfällungen des Polynoms $f(x)$ eintreten werden, wie sich dies auch dann erkennen lässt, wenn man etwa

$$M' \equiv |z_1, z_2, z_3, \ldots z_\varkappa \quad z_1,\ z_2 + \alpha_2,\ z_3 + \alpha_3,\ \ldots\ z_\varkappa + \alpha_\varkappa| \pmod p,$$
$$M'' \equiv |z_1, z_2, z_3, \ldots z_\varkappa \quad z_1,\ z_2,\ z_3 + \alpha_3,\ \ldots\ z_\varkappa + \alpha_\varkappa| \pmod p,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

setzt. Daher ist $\varkappa = \lambda$. Man erhält demnach als erstes Resultat:

Lehrsatz X. Die letzte Gruppe der Hauptreihe einer primitiven, auflösbaren Gleichung des Grades $p^\varkappa$ besteht aus den $p^\varkappa$ arithmetischen Substitutionen

$$t \equiv |z_1, z_2, \ldots z_\varkappa \quad z_1 + \alpha_1,\ z_2 + \alpha_2,\ \ldots\ z_\varkappa + \alpha_\varkappa| \pmod p.$$

Die Wurzeln der Gleichung werden dabei dargestellt durch

$$x_{z_1, z_2, \ldots z_\varkappa} \quad (z_\lambda = 0, 1, 2, \ldots p-1).$$

Da G, die Gruppe der Gleichung mit M vertauschbar ist, so folgt aus § 138, dass G aus der Kombination von arithmetischen und geometrischen Substitutionen bestehen wird. Es folgt damit als weiteres Resultat:

Lehrsatz XI. Die Gruppe G jeder auflösbaren, primitiven Gleichung des Grades $p^\varkappa$ besteht aus der Gruppe der arithmetischen Substitutionen des Grades $p^\varkappa$ kombiniert mit geometrischen Substitutionen desselben Grades

$$u \equiv | z_1, z_2, \ldots z_\varkappa \quad a_1 z_1 + b_1 z_2 + \ldots + c_1 z_\varkappa,\ a_2 z_1 + b_2 z_2 + \ldots + c_2 z_\varkappa,\ \ldots | \pmod{p}.$$

§ 239. Bevor wir in den allgemeineren Untersuchungen fortfahren, betrachten wir die Fälle $\varkappa = 1, 2$, trotzdem der erstere bereits früher besprochen und erledigt ist.

Wir betrachten zuerst die auflösbaren, primitiven Gleichungen des Primzahlgrades p. Das Wort „primitiv" können wir dabei aber unterdrücken, da die Imprimitivität eine Einteilung der Wurzeln in Systeme von gleichvielen Elementen fordern würde, welche ja hier unmöglich ist.

Die Gruppe der allgemeinsten auflösbaren Gleichung muss mit

$$G \equiv | z \quad az + \alpha | \quad (a = 1, 2, \ldots p-1;\ \alpha = 0, 1, \ldots p-1) \pmod{p}$$

zusammenfallen oder in ihr enthalten sein. Wir beweisen das erstere dadurch, dass wir die Gruppe der Zusammensetzung von G aus bis M konstruieren und zeigen, dass alle Faktoren der Zusammensetzung, welche dabei auftreten, Primzahlen sind. Wir zerlegen $p-1$ in seine Primfaktoren $p-1 = q_1 . q_2 \ldots$ und bilden die Untergruppe

$$H \equiv | z \quad a_1 q_1 . z + \alpha_1 | \quad \left(a_1 = 1, 2, \ldots \frac{p-1}{q_1};\ \alpha_1 = 0, 1, \ldots p-1\right),$$

ebenso die Untergruppe

$$J \equiv | z \quad a_2 q_1 q_2 . z + \alpha_2 | \quad \left(a_2 = 1, 2, \ldots \frac{p-1}{q_1 q_2};\ \alpha_2 = 0, 1, \ldots p-1\right),$$

und fahren so fort. Dann gehören H, J, ... der Hauptreihe von G an. Denn es ist z. B.

$$G^{-1} J G = J.$$

Setzt man nämlich

$$t \equiv | z \quad az + \alpha |, \text{ so folgt } t^{-1} \equiv \left| z \quad \frac{1}{a}(z - \alpha) \right|,$$

$$\left|z \quad \frac{1}{a}(z-\alpha)\right| \cdot \left|z \quad a_2 q_1 q_2 . z + \alpha_2\right| \cdot \left|z \quad az+\alpha\right|$$
$$\equiv \left|z \quad a_2 q_1 q_2 . z + \frac{a_2 q_1 q_2 \alpha - \alpha + \alpha_2}{a}\right|,$$

so dass die Transformation einer Substitution aus J durch eine beliebige Substitution aus G wiederum zu einer Substitution aus J führt. Offenbar stimmt hier die Hauptreihe mit der Reihe der Zusammensetzung überein; alle Faktoren der Zusammensetzung $q_1, q_2, \ldots$ sind Primzahlen. Damit ist der Nachweis vollendet.

Lässt eine Substitution von G zwei Wurzeln x_γ, x_δ ungeändert, so lässt dieselbe alle Wurzeln ungeändert. Denn aus $\gamma \equiv a\gamma + \alpha$, $\delta \equiv a\delta + \alpha$ folgt unzweideutig $a \equiv 1$, $\alpha \equiv 0$ und die Substitution wird zu der identischen $1 = |z \quad z|$.

Lässt eine Substitution von G eine Wurzel x_γ ungeändert und führt sie $x_{\gamma+1}$ in x_δ über, so geht jedes x_ε in $x_{(\delta-\gamma)(\varepsilon-\gamma)+\gamma}$ über. Denn aus $\gamma \equiv a\gamma + \alpha$, $\delta \equiv a(\gamma+1) + \alpha$ folgt unzweideutig $a \equiv \delta - \gamma$, $\alpha \equiv \gamma(\gamma - \delta + 1)$ und die betreffende Substitution erhält die Form $|z \quad (\delta-\gamma)z + \gamma(\gamma - \delta + 1)|$.

Lässt eine Substitution von G keine Wurzel ungeändert und wandelt sie x_γ in x_δ um, so geht x_ε in $x_{\varepsilon+\delta-\gamma}$ über. Denn nur dann kann für keinen Wert von γ die Kongruenz $\gamma \equiv a\gamma + \alpha$ stattfinden, wenn $a \equiv 1$ ist. Soll dabei $\gamma + 1$ in δ übergehen, so muss $\delta = \gamma + \alpha$ sein; dies ergiebt $\alpha = \delta - \gamma$ und für z die arithmetische Substitution $|z \quad z + \delta - \gamma|$.

Dies sind genau dieselben Resultate, welche uns früher die algebraische Methode lieferte.

Lehrsatz XII. Die allgemeinen auflösbaren Gleichungen vom Primzahlgrade p sind die Galois'schen Gleichungen. Ihre Gruppe hat die Ordnung $p(p-1)$; sie wird aus den Substitutionen der Form

$$s \equiv |z \quad az+\alpha|; \quad (a = 1, 2, \ldots p-1; \ \alpha = 0, 1, \ldots p-1) \pmod{p}$$

gebildet. Ihre Faktoren der Zusammensetzung sind alle Primzahlteiler von $(p-1)$, jeder so oft genommen, als er in $(p-1)$ als Faktor eingeht, und ausserdem p selbst.

§ 240. Wir gehen zu den allgemeinsten auflösbaren Gleichungen des Grades p^2 mit primitiver Gruppe über. Zu Grunde liegen die arithmetischen Substitutionen

$$t \equiv |z_1, z_2 \quad z_1 + \alpha_1, z_2 + \alpha_2| \pmod{p},$$

welche die letzte Gruppe M der Hauptreihe bilden. Um weiter zu der vorhergehenden Gruppe L der Reihe zu gehen, müsste man eine Substitution von folgenden Eigenschaften bestimmen: ihre Form ist

$$s \equiv |z_1, z_2 \quad a_1 z_1 + b_1 z_2, \; a_2 z_1 + b_2 z_2| \pmod{p};$$

die niedrigste Potenz derselben, welche in M vorkommt und also die Form t besitzt, muss eine Primzahl zum Exponenten haben. Da nun alle Potenzen von s wiederum dieselbe Form besitzen, wie s selbst, so muss die Potenz gleich $|z_1, z_2 \quad z_1, z_2| = 1$ werden, d. h. die Ordnung der Substitution s muss eine Primzahl werden.

Durch diese und ähnliche Prinzipien gelangt man zu den nachstehenden Resultaten,* auf deren Ableitung wir nicht näher eingehen:

Lehrsatz XIII. Von allgemeinen auflösbaren, primitiven Gleichungen des Grades p^2 giebt es drei verschiedene Typen.

Der erste Typus ist durch eine Gruppe der Ordnung $2.p^2(p-1)^2$ charakterisiert, deren Substitutionen aus den folgenden abgeleitet sind:

$$\begin{array}{ll} |z_1, z_2 \quad z_1 + \alpha_1, \; z_2 + \alpha_2| & (\alpha_1, \alpha_2 \equiv 0, 1, 2, \ldots p-1), \\ |z_1, z_2 \quad a_1 z_1, \; a_2 z_2| & (a_1, a_2 \equiv 1, 2, 3, \ldots p-1), \\ |z_1, z_2 \quad z_2, z_1|. & \end{array} \pmod{p},$$

Die zum zweiten Typus gehörigen Gruppen haben die Ordnung $2p^2(p^2-1)$ und ihre Substitutionen entstehen aus der Kombination der folgenden:

$$\begin{array}{ll} |z_1, z_2 \quad z_1 + \alpha_1, \; z_2 + \alpha_2| & (\alpha_1, \alpha_2 \equiv 0, 1, 2, \ldots p-1), \\ |z_1, z_2 \quad az_1 + bez_2, \; bz_1 + az_2| & (a, b \equiv 0, 1, \ldots p-1; \text{ nur nicht } a, b \equiv 0), \\ |z_1, z_2 \quad z_1, -z_2|; & \end{array}$$

e ist ein beliebiger quadratischer Rest mod. p.

Der dritte Typus besitzt Gruppen von der Ordnung $24p^2(p-1)$. Die Form der konstituierenden Substitutionen ist verschieden, jenachdem $p \equiv 1$ oder $p \equiv 3 \pmod{4}$ wird. Tritt das erstere ein, so kommen zu den beiden Substitutionen:

$$\begin{array}{ll} |z_1, z_2 \quad z_1 + \alpha_1, \; z_2 + \alpha_2| & (\alpha_1, \alpha_2 \equiv 0, 1, 2, \ldots p-1), \\ |z_1, z_2 \quad az_1, \; az_2| & (a \equiv 1, 2, 3, \ldots p-1) \end{array}$$

noch folgende vier, bei denen i eine Wurzel der Kongruenz $i^2 \equiv -1 \pmod{p}$ bedeutet:

* C. Jordan: Liouville, Journal de Mathém. (2) XIII, p. 111–135.

$$|z_1, z_2 \quad iz_1, -iz_2|, \qquad |z_1, z_2 \quad iz_2, iz_1|,$$
$$|z_1, z_2 \quad z_1 - iz_2, z_1 + iz_2|, \qquad |z_1, z_2 \quad z_1 + z_2, z_1 - z_2|.$$

Ist $p \equiv 3 \pmod 4$, so kommen zu jenen beiden noch folgende vier, bei denen s, t die Kongruenz $s^2 + t^2 \equiv -1 \pmod p$ befriedigen:

$$|z_1, z_2 \quad z_2, -z_1|, \qquad |z_1, z_2 \quad sz_1 + tz_2, \; tz_1 - sz_2|,$$
$$|z_1, z_2 \quad -(1+st)z_1 + (s-t^2)z_2, \; (t+s^2)z_1 + (st-s-t)z_2|,$$
$$|z_1, z_2 \quad sz_1 + (1+t)z_2, \; (t-1)z_1 - sz_2|.$$

Für $p = 3$ sind der erste und der zweite Typus, für $p = 5$ ist der zweite Typus nicht allgemein. Sie treten dabei als Spezialfälle des dritten auf, welcher stets allgemein ist.

§ 241. Wir kehren zu allgemeineren Betrachtungen zurück.

Genau wie im vorigen Paragraphen bei p^2, so können wir auch allgemein den Schluss auf diejenigen Substitutionen machen, welche der Gruppe L angehören, wo L die der Gruppe M in der Reihe der Zusammensetzung vorangehende Gruppe ist. L wird gebildet, wenn man zu den Substitutionen

$$t \equiv |z_1, z_2, \ldots z_\varkappa \quad z_1 + \alpha_1, \; z_2 + \alpha_2, \; \ldots z_\varkappa + \alpha_\varkappa| \pmod p$$

von M noch eine Substitution

$$s \equiv |z_1, z_2, \ldots \quad a_1 z_1 + b_1 z_2 + \ldots + c_1 z_\varkappa, \; a_2 z_1 + b_2 z_2 + \ldots + c_2 z_\varkappa, \ldots| \pmod p$$

hinzunimmt, bei der eine Primzahlpotenz die erste ist, die in die Form t tritt. Da alle Potenzen von s dieselbe Form wie s haben, so muss jene Potenz, die auch als Substitution t erscheint, gleich der Einheit werden; also erhalten wir die Bedingung, es müsse s eine Primzahl als Ordnung besitzen. Ferner darf die Gruppe $L = \{t, s\}$ nicht imprimitiv werden.

§ 242. Aus der Form der für G überhaupt möglichen Substitutionen erkennt man:

Lehrsatz XIV. Alle Substitutionen, mit Ausnahme der Einheit, welche der Gruppe

$$M = |z_1, z_2, \ldots z_\varkappa \quad z_1 + \alpha_1, \; z_2 + \alpha_2, \; \ldots z_\varkappa + \alpha_\varkappa|$$

angehören, setzen alle Wurzeln der Gleichung um.

Umkehren lässt sich dieser Satz, wie es bei $\varkappa = 1$ möglich war, im allgemeinen Falle nicht. Denn das Element $x_{z_1, z_2, \ldots z_\varkappa}$ bleibt für

$$s = |z_1, z_2, \ldots z_\varkappa \quad a_1 z_1 + b_1 z_1 + \ldots + c_1 z_\varkappa + \alpha_1, \; a_2 z_1 + b_2 z_2 + \ldots + c_1 z_\varkappa + \alpha_2, \ldots|$$

nur ungeändert, falls die $\varkappa$ Kongruenzen (mod. p)

$$S) \quad \begin{cases} (a_1-1)z_1 + b_1 z_2 + \ldots + c_1 z_\varkappa + \alpha_1 \equiv 0 \\ a_2 z_1 + (b_2-1)z_2 + \ldots + c_2 z_\varkappa + \alpha_2 \equiv 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_\varkappa z_1 + b_\varkappa z_2 + \ldots + (c_\varkappa - 1) z_\varkappa + \alpha_\varkappa \equiv 0 \end{cases} \pmod p$$

befriedigt sind; sobald daher die Determinante

$$D = \begin{vmatrix} a_1-1, & b_1, & \ldots & c_1 \\ a_2, & b_2-1, & \ldots & c_2 \\ \cdots & \cdots & \cdots & \cdots \\ a_\varkappa, & b_\varkappa, & \ldots & c_\varkappa - 1 \end{vmatrix} \equiv 0 \pmod p$$

ist, lassen sich $\alpha_1, \alpha_2, \ldots \alpha_\varkappa$ so wählen, dass das System S) für kein System $z_1, z_2, \ldots z_\varkappa$ befriedigt wird.

Wir betrachten jetzt alle Substitutionen unserer Gruppe G, welche ein Element ungeändert lassen. Da die Elemente sich nur durch ihre Benennung von einander unterscheiden, so können wir $x_{0,0,\ldots 0}$ als das feste Element ansehen. Dann sind die Substitutionen, welche dieses Element nicht umsetzen,

$$\Gamma = | z_1, z_2, \ldots z_\varkappa \quad a_1 z_1 + b_1 z_2 + \ldots + c_1 z_\varkappa, \; a_2 z_1 + b_2 z_2 + \ldots + c_2 z_\varkappa, \ldots |.$$

Auf diese reduziert sich die Gruppe, falls man $x_{0,0,\ldots 0}$ der Gleichung adjungiert. Da alle Substitutionen von G erhalten werden, wenn man zu denen von Γ die konstanten Grössen von $\alpha_1, \alpha_2, \ldots$ hinzufügt, und da die Wahl der α auf $p^\varkappa$ Arten möglich ist, so erkennt man, dass durch Adjungierung einer einzigen Wurzel G auf den $p^{\varkappa\text{ten}}$ Teil seiner Substitutionen reduziert wird.

§ 243. Wir wollen ferner annehmen, dass eine Substitution der Gruppe $(\varkappa+1)$ Elemente $x_{z_1, z_2, \ldots z_\varkappa}$ ungeändert lasse. Dann ist das System S) des vorigen Paragraphen für $(\varkappa+1)$ Wertsystem von $z_1, z_2, \ldots z_\varkappa$

$$z_1 = \xi_1^{(\lambda)}, \quad z_2 = \xi_2^{(\lambda)}, \ldots z_\varkappa = \xi_\varkappa^{(\lambda)} \qquad (\lambda = 0, 1, 2, \ldots \varkappa)$$

erfüllt. Wir wollen jetzt aber nicht die Koefficienten $a, b, \ldots c$; α der Substitution, sondern die Werte $\xi_1^{(\lambda)}, \xi_2^{(\lambda)}, \ldots \xi_\varkappa^{(\lambda)}$ als gegeben ansehen und die Substitution zu bestimmen suchen. Ist dann die Lösungsdeterminante

$$E = \begin{vmatrix} \xi_1, & \xi_2, & \ldots & \xi_\varkappa, & 1 \\ \xi_1', & \xi_2', & \ldots & \xi_\varkappa', & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \xi_1^{(\varkappa)}, & \xi_2^{(\varkappa)}, & \ldots & \xi_\varkappa^{(\varkappa)}, & 1 \end{vmatrix}$$

nicht kongruent 0 (mod. p), so giebt es für die $\varkappa$ Systeme T_1), T_2), $\ldots$ $T_\varkappa$) von je $(\varkappa+1)$ Kongruenzen mit den Unbekannten $a, b, \ldots$; α

$$
\begin{aligned}
&T_1) \quad (a_1-1)\xi_1^{(\lambda)} + \quad b_1\xi_2^{(\lambda)} + \ldots + \quad c_1\xi_\varkappa^{(\lambda)} + \alpha_1 \equiv 0,\\
&T_2) \quad a_2\xi_1^{(\lambda)} + (b_2-1)\xi_2^{(\lambda)} + \ldots + c_2\xi_\varkappa^{(\lambda)} + \alpha_2 \equiv 0, \qquad (\lambda = 0,1,2,\ldots\varkappa)\\
&\qquad\qquad \ldots\ldots\ldots\ldots\ldots\ldots\\
&T_\varkappa) \quad a_\varkappa\xi_1^{(\lambda)} + \quad b_\varkappa\xi_2^{(\lambda)} + \ldots + (c_\varkappa-1)\xi_\varkappa^{(\lambda)} + \alpha_\varkappa \equiv 0
\end{aligned}
$$

nur je eine Lösung, nämlich entsprechend

$$
\begin{aligned}
&L_1) \quad a_1 = 1, \quad b_1 = 0, \ldots c_1 = 0; \quad \alpha_1 = 0,\\
&L_2) \quad a_2 = 0, \quad b_2 = 1, \ldots c_2 = 0; \quad \alpha_2 = 0,\\
&\qquad\qquad \ldots\ldots\ldots\ldots\ldots\\
&L_\varkappa) \quad a_\varkappa = 0, \quad b_\varkappa = 0, \ldots c_\varkappa = 1; \quad \alpha_\varkappa = 0,
\end{aligned}
$$

und diese Lösungen liefern vereint die identische Substitution 1.

Wir nennen nun ein System von $(\varkappa+1)$ Wurzeln unserer Gleichung, für welche $E \equiv 0 \pmod{p}$ ist, ein System konjugierter Wurzeln.

Dann folgt der Satz:

Lehrsatz XV. Wenn eine Substitution einer primitiven auflösbaren Gruppe vom Grade $p^\varkappa$ so beschaffen ist, dass sie $(\varkappa+1)$ Wurzeln ungeändert lässt, welche kein konjugiertes System bilden, so reduziert sie sich auf die identische Substitution 1.

Adjungiert man daher der Gleichung $(\varkappa+1)$ solcher Wurzeln, so reduziert sich die Gruppe G der Gleichung auf diejenigen Substitutionen, welche die $(\varkappa+1)$ Wurzeln ungeändert lassen, d. h. auf die Substitution 1. Dadurch ist die Gleichung gelöst.

Lehrsatz XVI. Alle Wurzeln einer auflösbaren primitiven Gleichung des Grades $p^\varkappa$ sind durch $(\varkappa+1)$ unter ihnen rational darstellbar, falls dieselben kein konjugiertes System bilden.

Setzen wir, was erlaubt ist, da es durch Änderung der Indicesbezeichnung erlangt werden kann, die eine der Wurzeln gleich $x_{0,0,\ldots 0}$, so wird die Determinante

$$
\pm E = \begin{vmatrix} \xi_1', & \xi_2', & \ldots & \xi_\varkappa' \\ \cdot & \cdot & \cdot & \cdot \\ \xi_1^{(\varkappa)}, & \xi_2^{(\varkappa)}, & \ldots & \xi_\varkappa^{(\varkappa)} \end{vmatrix}.
$$

Sollen die Wurzeln kein konjugiertes System bilden, so darf E nicht $\equiv 0 \pmod{p}$ sein. Die Anzahl r der Wurzelsysteme, welche dieser Bedingung genügt, ist in den §§ 140–142 (S. 154, 155) bestimmt. Wir fanden

$$
r = (p^\varkappa - 1)(p^\varkappa - p)(p^\varkappa - p^2) \ldots (p^\varkappa - p^{\varkappa-1}).
$$

Lehrsatz XVII. Zu jeder Wurzel $x_{z_1, z_2, \ldots z_\varkappa}$ lassen sich

$$\frac{(p^\varkappa - 1)(p^\varkappa - p) \ldots (p^\varkappa - p^{\varkappa-1})}{1.2. \ldots \varkappa}$$

Systeme von $\varkappa$ Wurzeln derart bestimmen, dass die $(\varkappa+1)$ Wurzeln kein konjugiertes System bilden und also im stande sind, jede andere Wurzel rational darzustellen. Das System der $(\varkappa+1)$ Wurzeln

$$x_{0,0,0,\ldots 0}, \quad x_{1,0,0,\ldots 0}, \quad x_{0,1,0,\ldots 0}, \quad \ldots \quad x_{0,0,0,\ldots 1}$$

ist zur rationalen Darstellung aller Wurzeln geeignet.

Diese Resultate werfen ein neues Licht auf unsere früheren Untersuchungen über Tripelgleichungen, speziell auf die Lösung der Hesse'schen Gleichung neunten Grades (vergl. §§ 198, 199). Man erkennt, dass wir in gleicher Weise auflösbare Quadrupelgleichungen vom Grade p^3 konstruieren könnten u. s. f.