



UNIVERSITÄTSBIBLIOTHEK
HEIDELBERG

HEIDELBERGER AKADEMIE
DER WISSENSCHAFTEN



Heidelberger Akademie der Wissenschaften

Mathematische Abhandlungen

Autor: **Loewy, Alfred** (1873 – 1935)

Titel: **Neue elementare Begründung und Erweiterung
der Galoisschen Theorie : (Fortsetzung)**

Sitzungsberichte der Heidelberger Akademie der Wissenschaften,
Mathematisch-naturwissenschaftliche Klasse ; 1927, 1

Signatur UB Heidelberg: L 1086-20

In Fortsetzung seiner Untersuchungen über die zu endlichen algebraischen Körpern gehörigen Transmutationssysteme führt der Verfasser den neuen Begriff „Quotientenmischgruppe“ ein und untersucht insbesondere die P-Transmutationssysteme, die mit der Imprimitivität der Gleichungstheorie nahe zusammenhängen.

(Zsfassung aus: Sitzungsberichte der Heidelberger Akademie der Wissenschaften / Jahreshft 1926/27, S. VII)

Sitzungsberichte
der Heidelberger Akademie der Wissenschaften
Stiftung Heinrich Lanz

Mathematisch-naturwissenschaftliche Klasse

==== Jahrgang 1927. 1. Abhandlung. =====

Neue elementare Begründung und Erweiterung der Galoisschen Theorie

(Fortsetzung)

Von

Alfred Loewy
in Freiburg i. B.

Eingegangen am 30. Oktober 1926



Berlin und Leipzig 1927.

Walter de Gruyter & Co.

vormals G. J. Göschen'sche Verlagshandlung / J. Guttentag, Verlags-
buchhandlung / Georg Reimer / Karl J. Trübner / Veit & Comp.

H 95⁶

Neue elementare Begründung und Erweiterung der Galoisschen Theorie.

(Fortsetzung.¹⁾)

§ 5.

Zu dem Transmutationssystem $\mathfrak{S}$ der Dirigenten $\varrho_1, \varrho_2, \dots, \varrho_k$ des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ und seinen Quotientenmischgruppen isomorphe Transmutationssysteme rationaler Funktionen von $\varrho_1, \varrho_2, \dots, \varrho_k$. Die irreduzible Gleichung für eine primitive Funktion des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ und ihr Zusammenhang mit dem Transmutationssystem $\mathfrak{S}$.

Zunächst entnehme ich für die folgenden Betrachtungen einem Aufsatz, der im Jubiläumsband des Journals für die reine und angewandte Mathematik anlässlich dessen hundertjährigen Bestehens erscheint, die Begriffe des abstrakten Transmutationssystems oder, wie ich auch sage, der Mischgruppe, weiter der Quotientenmischgruppe und des Isomorphismus zweier Transmutationssysteme. Eine Mischgruppe $\mathfrak{T}$ besteht aus zwei Gattungen von Elementen: $\mathfrak{G}$ und $\mathfrak{H}$. Die Elemente von $\mathfrak{G}$ bilden eine Gruppe, die größte in $\mathfrak{T}$ enthaltene Gruppe, den Kern von $\mathfrak{T}$; die Elemente H von $\mathfrak{H}$, der Schale von $\mathfrak{T}$, lassen sich als rechtshändige Faktoren mit jedem Element von $\mathfrak{G}$ komponieren und besitzen inverse Elemente H^{-1} , so daß stets das Produkt HH^{-1} gebildet werden kann und gleich E_1 ist, wobei E_1 das Einheits-element von $\mathfrak{G}$ bedeutet. Die Elemente H^{-1} brauchen nicht der Mischgruppe $\mathfrak{T}$ anzugehören.

Die wesentliche Eigenschaft einer Mischgruppe $\mathfrak{T}$ ist, daß sie sich nach ihrem Kern $\mathfrak{G}$ zerlegen läßt in

$$\mathfrak{T} = \mathfrak{G} + \mathfrak{G}H_2 + \mathfrak{G}H_3 + \dots,$$

wobei die Komplexe $\mathfrak{G}, \mathfrak{G}H_2, \mathfrak{G}H_3, \dots$ untereinander elementenfremd sind.

Das Transmutationssystem $\mathfrak{S}$ der Dirigenten $\varrho_1, \varrho_2, \dots, \varrho_k$ des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ ist, wie man unmittelbar sieht, eine Mischgruppe im definierten Sinne, und zwar hier eine endliche, d. h. eine solche mit einer endlichen Anzahl von Transmutationen.

¹⁾ Die ersten vier Paragraphen dieser Arbeit sind erschienen in diesen Sitzungsberichten Jahrgang 1925, Abhandlung 7, zitiert mit I.

Der Kern von $\mathfrak{S}$ ist die in $\mathfrak{S}$ enthaltene maximale automorphe Untergruppe $\mathfrak{S}_a^{(m)}$ der Dirigenten $\varrho_1, \varrho_2, \dots, \varrho_k$ des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ [vgl. Satz 1 des § 4 (I S. 37)], und man hat die Zerlegung $\mathfrak{S} = \mathfrak{S}_a^{(m)} + \mathfrak{S}_a^{(m)} P_2 + \mathfrak{S}_a^{(m)} P_3 + \dots + \mathfrak{S}_a^{(m)} P_{t_n}$ [Satz 2 des § 4 (I S. 39)].

Ist $\mathfrak{U}$ irgendeine im Kern $\mathfrak{G}$ einer Mischgruppe $\mathfrak{I}$ enthaltene Untergruppe, so bestimmt $\mathfrak{U}$ eine neue Mischgruppe. Das neue Transmutationssystem bezeichne ich mit $\mathfrak{I}|\mathfrak{U}|$ und nenne es die Quotientenmischgruppe $\mathfrak{I}|\mathfrak{U}|$. Die Elemente dieser Mischgruppe sind die Komplexe, die sich bei der Zerlegung der Mischgruppe $\mathfrak{I}$ nach der im Kern $\mathfrak{G}$ von $\mathfrak{I}$ befindlichen Untergruppe $\mathfrak{U}$ ergeben; ebenso wie man $\mathfrak{I}$ nach seinem Kern $\mathfrak{G}$ zerlegen kann, läßt sich $\mathfrak{I}$ auch durch Fortführung der Zerlegung nach jeder in $\mathfrak{G}$ enthaltenen Untergruppe $\mathfrak{U}$ zerlegen.¹⁾ Zur näheren Untersuchung von $\mathfrak{I}|\mathfrak{U}|$ betrachten wir die Gesamtheit derjenigen Elemente N des Kernes $\mathfrak{G}$ von $\mathfrak{I}$, die mit $\mathfrak{U}$ vertauschbar sind, für die also $\mathfrak{U}N = N\mathfrak{U}$ ist; diese Elemente bilden eine Gruppe $\mathfrak{N}$, den sogenannten Normalisator von $\mathfrak{U}$ — die größte Untergruppe von $\mathfrak{G}$, in der $\mathfrak{U}$ invariant ist.

Wir zerlegen $\mathfrak{I}$ nach der in $\mathfrak{I}$ enthaltenen Untergruppe $\mathfrak{N}$ und erhalten

$$(1) \quad \mathfrak{I} = \mathfrak{N} + \mathfrak{N}P_2 + \mathfrak{N}P_3 + \dots + \mathfrak{N}P_p,$$

wobei $P_2, P_3, \dots, P_p$ Elemente aus $\mathfrak{I}$ bedeuten und die Komplexe $\mathfrak{N}, \mathfrak{N}P_2, \mathfrak{N}P_3, \dots, \mathfrak{N}P_p$ untereinander elementenfremd sind. Durch Zerlegung der Gruppe $\mathfrak{N}$ nach ihrer Untergruppe $\mathfrak{U}$ ergebe sich:

$$(2) \quad \mathfrak{N} = \mathfrak{U} + \mathfrak{U}N_2 + \mathfrak{U}N_3 + \dots + \mathfrak{U}N_n.$$

Dann besteht für $\mathfrak{I}$ die folgende Zerlegung (3) nach $\mathfrak{U}$:

$$(3) \quad \begin{aligned} \mathfrak{I} = & \mathfrak{U} + \mathfrak{U}N_2 + \mathfrak{U}N_3 + \dots + \mathfrak{U}N_n + \\ & \mathfrak{U}P_2 + \mathfrak{U}N_2P_2 + \mathfrak{U}N_3P_2 + \dots + \mathfrak{U}N_nP_2 + \\ & \vdots \\ & \mathfrak{U}P_p + \mathfrak{U}N_2P_p + \mathfrak{U}N_3P_p + \dots + \mathfrak{U}N_nP_p, \end{aligned}$$

wobei die Elemente von $\mathfrak{I}|\mathfrak{U}|$ die auf der rechten Seite von (3)

¹⁾ Ist $\mathfrak{I}$ selbst eine Gruppe, besteht also $\mathfrak{I}$ nur aus Elementen seines Kernes $\mathfrak{G}$, so sind die Elemente von $\mathfrak{I}|\mathfrak{U}|$ in der Terminologie des Lehrbuches der Algebra von H. Weber (Bd. 2, S. 8, Braunschweig, 2. Auflage, 1899) $\mathfrak{U}$ und seine Nebengruppen. Ist $\mathfrak{I} = \mathfrak{G}$ und ist außerdem noch $\mathfrak{U}$ invariante Untergruppe von $\mathfrak{G}$, fällt also der Normalisator $\mathfrak{N}$ von $\mathfrak{U}$ mit $\mathfrak{G} = \mathfrak{I}$ zusammen, so geht $\mathfrak{I}|\mathfrak{U}|$ in die von C. Jordan (Bulletin de la soc. de France, 1, 46 [1873]) in die Wissenschaft eingeführte und von O. Hölder (Math. Annalen 34, 33 [1889]) wiedergefundene Quotientengruppe $\mathfrak{G}|\mathfrak{U}|$ über.

stehenden np Komplexe $\mathfrak{U} N_i P_j$ ($i = 1, 2, \dots, n; j = 1, 2, \dots, p$) sind und $N_1 = P_1$ das Einheitselement E_1 von $\mathfrak{G}$ bedeutet. Sind $\mathfrak{U} N_i$ und $\mathfrak{U} N_k$ zwei Komplexe, die in der ersten Zeile auf der rechten Seite von (3) stehen, so ist $(\mathfrak{U} N_i) (\mathfrak{U} N_k) = \mathfrak{U} (N_i \mathfrak{U}) N_k = \mathfrak{U} (\mathfrak{U} N_i) N_k = (\mathfrak{U} \mathfrak{U}) N_i N_k = \mathfrak{U} N_i N_k = \mathfrak{U} N_j$, wobei $N_j = N_i N_k$ wegen des Gruppencharakters von $\mathfrak{N}$ ein Element aus $\mathfrak{N}$, also $\mathfrak{U} N_j$ ein Komplex aus der ersten Zeile von (3) ist. Die Komplexe der ersten Zeile von (3) bilden also eine Gruppe, die Quotientengruppe $\mathfrak{N} | \mathfrak{U}$; diese ist der Kern von $\|\mathfrak{I} | \mathfrak{U}\|$.

Irgendein Transmutationssystem $\mathfrak{I}^*$ heißt zu der Quotientenmischgruppe $\|\mathfrak{I} | \mathfrak{U}\|$ isomorph, wenn $\mathfrak{I}^*$ aus np Elementen besteht und der Kern von $\mathfrak{I}^*$ eine zu dem Kern von $\|\mathfrak{I} | \mathfrak{U}\|$ (das ist die Quotientengruppe $\mathfrak{N} | \mathfrak{U}$) isomorphe Gruppe ist. Dann läßt sich $\mathfrak{I}^*$ in der Form schreiben:

$$(3^*) \quad \begin{aligned} \mathfrak{I}^* = & T_1^* + T_2^* + \dots + T_n^* + \\ & T_1^* P_2^* + T_2^* P_2^* + \dots + T_n^* P_2^* + \\ & \vdots \\ & T_1^* P_p^* + T_2^* P_p^* + \dots + T_n^* P_p^*, \end{aligned}$$

wobei die Elemente $T_1^*, T_2^*, \dots, T_n^*$ eine Gruppe bilden, den Komplexen $\mathfrak{N}, \mathfrak{N} \mathfrak{U}_2, \dots, \mathfrak{N} \mathfrak{U}_n$ entsprechen und die Zuordnung so beschaffen ist, daß, wenn T_i^* und $\mathfrak{U} N_i$, T_k^* und $\mathfrak{U} N_k$ Partner voneinander sind, dies auch stets für die Produkte $T_i^* T_k^* = T_j^*$ und $(\mathfrak{U} N_i) (\mathfrak{U} N_k) = \mathfrak{U} N_i N_k = \mathfrak{U} N_j$ zutrifft. Ordnet man den Elementen $T_k^* P_l^*$ ($k = 1, 2, \dots, n; l = 2, 3, \dots, p$) von $\mathfrak{I}^*$ die Komplexe $\mathfrak{U} N_k P_l$ von $\|\mathfrak{I} | \mathfrak{U}\|$ zu, so hat man $(\mathfrak{U} N_i) (\mathfrak{U} N_k P_l) = \mathfrak{U} \mathfrak{U} N_i N_k P_l = \mathfrak{U} N_i N_k P_l = \mathfrak{U} N_j P_l$ und diesem Komplex entspricht kraft unserer Zuordnung $T_j^* P_l^* = T_i^* T_k^* P_l^* = (T_i^*) (T_k^* P_l^*)$, also das Produkt jener Elemente, die den Komplexen $\mathfrak{U} N_i$ und $\mathfrak{U} N_k P_l$ zugeordnet sind.

Für das Folgende ist es noch erforderlich, einen weiteren Begriff einzuführen, nämlich den des Hyperisomorphismus der Mischgruppe $\mathfrak{I}^*$ mit der Quotientenmischgruppe $\|\mathfrak{I} | \mathfrak{U}\|$. Die Mischgruppe $\mathfrak{I}^*$ soll zu $\|\mathfrak{I} | \mathfrak{U}\|$ hyperisomorph heißen, wenn $\mathfrak{I}^*$ aus np Elementen besteht, die Elemente $T_1^*, T_2^*, \dots, T_n^*$ eine zu dem Kern von $\|\mathfrak{I} | \mathfrak{U}\|$, der Quotientengruppe $\mathfrak{N} | \mathfrak{U}$ isomorphe Gruppe bilden, ohne daß die Elemente $T_1^*, T_2^*, \dots, T_n^*$ notwendig den Kern von $\mathfrak{I}^*$ erschöpfen müssen, die Elemente $T_1^*, T_2^*, \dots, T_n^*$ brauchen also im Falle des Hyperisomorphismus eventuell nur eine Untergruppe des Kerns von $\mathfrak{I}^*$ zu bilden. Ist $\mathfrak{I}^*$ hyperisomorph zu $\|\mathfrak{I} | \mathfrak{U}\|$, so können demnach die np Elemente von $\mathfrak{I}^*$ sich gegebenenfalls in umfassenderer Weise komponieren lassen, als dies für die auf der rechten Seite von (3) stehenden Komplexe, die Elemente von $\|\mathfrak{I} | \mathfrak{U}\|$, zutrifft.

Ist im besonderen $\mathfrak{U} = E_1$, wobei E_1 das Einheitsselement der Mischgruppe $\mathfrak{I}$ bedeutet, so heißen die Mischgruppen $\mathfrak{I}^*$ und $\mathfrak{I}$ isomorph beziehungsweise $\mathfrak{I}^*$ hyperisomorph zu $\mathfrak{I}$.

Wir beweisen nunmehr den für das folgende grundlegenden

Satz 1.¹⁾ $\mathfrak{S}$ sei das Transmutationssystem der Dirigenten $\varrho_1, \varrho_2, \dots, \varrho_k$ des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$. Weiter bedeute $\mathfrak{S}_a$ eine Untergruppe von $\mathfrak{S}_a^{(m)}$, der maximalen automorphen Untergruppe des Transmutationssystems $\mathfrak{S}$. Ist $\sigma_1(\varrho_1, \varrho_2, \dots, \varrho_k), \sigma_2(\varrho_1, \varrho_2, \dots, \varrho_k), \dots, \sigma_l(\varrho_1, \varrho_2, \dots, \varrho_k)$ ein System rationaler Funktionen von $\varrho_1, \varrho_2, \dots, \varrho_k$ mit Koeffizienten aus P , die sämtlich bei allen Transmutationen von $\mathfrak{S}_a$ ihre Werte nicht ändern, von denen aber bei jeder $\mathfrak{S}_a$ nicht angehörigen Transmutation aus $\mathfrak{S}$ mindestens eine Funktion ihren Wert verändert, so ist das Transmutationssystem Σ der Dirigenten $\sigma_1, \sigma_2, \dots, \sigma_l$ des Körpers $(P; \sigma_1, \sigma_2, \dots, \sigma_l)$ hyperisomorph zu dem Transmutationssystem, das die Quotientenmischgruppe $\mathfrak{S} \mathfrak{S}_a$ bestimmt.

Unser Satz besagt: Das Transmutationssystem Σ besitzt eine automorphe Untergruppe Σ_a . Ist $\mathfrak{N}$ der Normalisator, den $\mathfrak{S}_a$ innerhalb der maximalen automorphen Untergruppe $\mathfrak{S}_a^{(m)}$ des Transmutationssystems $\mathfrak{S}$ besitzt, besteht also $\mathfrak{N}$ aus der Gesamtheit aller automorphen Transmutationen von $\mathfrak{S}$, die mit $\mathfrak{S}_a$ vertauschbar sind, und lauten die GALOISSchen Zerlegungen der Gruppe $\mathfrak{N}$ nach ihrer invarianten Untergruppe $\mathfrak{S}_a$ und des Transmutationssystems $\mathfrak{S}$ nach seiner automorphen Untergruppe $\mathfrak{N}$

$$(1) \quad \mathfrak{S} = \mathfrak{N} + \mathfrak{N}P_2 + \mathfrak{N}P_3 + \dots + \mathfrak{N}P_p \text{ beziehungsweise}$$

$$(2) \quad \mathfrak{N} = \mathfrak{S}_a + \mathfrak{S}_a N_2 + \mathfrak{S}_a N_3 + \dots + \mathfrak{S}_a N_n,$$

so enthält Σ_a die n Transmutationen

$$\left(\begin{smallmatrix} \sigma_1 \\ (\sigma_1) \end{smallmatrix} \mathfrak{S}_a N_i \begin{smallmatrix} \sigma_2 \\ (\sigma_2) \end{smallmatrix} \mathfrak{S}_a N_i \dots \begin{smallmatrix} \sigma_l \\ (\sigma_l) \end{smallmatrix} \mathfrak{S}_a N_i \right) (i = 1, 2, \dots, n),$$

wobei $N_1 = E_1 = \begin{pmatrix} \varrho_1 & \varrho_2 & \dots & \varrho_k \\ \varrho_1 & \varrho_2 & \dots & \varrho_k \end{pmatrix}$ bedeutet, und ist isomorph zu der Quotientengruppe $\mathfrak{N} \mathfrak{S}_a$. Die weiteren Transmutationen von Σ haben die Form:

$$\left(\begin{smallmatrix} \sigma_1 \\ (\sigma_1) \end{smallmatrix} \mathfrak{S}_a N_i P_j \begin{smallmatrix} \sigma_2 \\ (\sigma_2) \end{smallmatrix} \mathfrak{S}_a N_i P_j \dots \begin{smallmatrix} \sigma_l \\ (\sigma_l) \end{smallmatrix} \mathfrak{S}_a N_i P_j \right) (i = 1, 2, \dots, n; j = 2, 3, \dots, p).$$

¹⁾ Die Bezeichnung knüpft an Satz 6 aus I, S. 48 an. Für $\mathfrak{I}$ und $\mathfrak{U}$ haben wir in (1) und (2) $\mathfrak{S}$ und $\mathfrak{S}_a$ gesetzt.

Aus dem automorphen Charakter von Σ_a folgt die Existenz von ln rationalen Funktionen $R_{hi}(\sigma_1, \sigma_2, \dots, \sigma_l)$ von $\sigma_1, \sigma_2, \dots, \sigma_l$ ($h = 1, 2, \dots, l; i = 1, 2, \dots, n$) mit Koeffizienten aus P , so daß

$$(4) \quad \begin{cases} (\sigma_1) \mathfrak{S}_a N_i = R_{1i}(\sigma_1, \sigma_2, \dots, \sigma_l), \\ (\sigma_2) \mathfrak{S}_a N_i = R_{2i}(\sigma_1, \sigma_2, \dots, \sigma_l), \\ \vdots \\ (\sigma_l) \mathfrak{S}_a N_i = R_{li}(\sigma_1, \sigma_2, \dots, \sigma_l), \\ (i = 1, 2, \dots, n) \end{cases}$$

ist.

Daß das Transmutationssystem Σ aus den $n p$ Transmutationen

$$\left(\begin{smallmatrix} \sigma_1 \\ (\sigma_1) \end{smallmatrix} \mathfrak{S}_a N_i P_j \begin{smallmatrix} \sigma_2 \\ (\sigma_2) \end{smallmatrix} \mathfrak{S}_a N_i P_j \dots \begin{smallmatrix} \sigma_l \\ (\sigma_l) \end{smallmatrix} \mathfrak{S}_a N_i P_j \right)$$

($i = 1, 2, \dots, n; j = 1, 2, \dots, p$) besteht, die der aus den Relationen (1) und (2) zu entnehmenden GALOISSchen Zerlegung

$$\begin{aligned} (\bar{3}) \quad \mathfrak{S} = & \mathfrak{S}_a + \mathfrak{S}_a N_2 + \mathfrak{S}_a N_3 + \dots + \mathfrak{S}_a N_n + \\ & \mathfrak{S}_a P_2 + \mathfrak{S}_a N_2 P_2 + \mathfrak{S}_a N_3 P_2 + \dots + \mathfrak{S}_a N_n P_2 + \\ & \vdots \\ & \mathfrak{S}_a P_p + \mathfrak{S}_a N_2 P_p + \mathfrak{S}_a N_3 P_p + \dots + \mathfrak{S}_a N_n P_p \end{aligned}$$

entsprechen, ergibt sich aus Satz 6 des § 4 (I Seite 48). Die Funktionen $(\sigma_1) \mathfrak{S}_a N_i, (\sigma_2) \mathfrak{S}_a N_i, \dots, (\sigma_l) \mathfrak{S}_a N_i$ bleiben bei den Transmutationen von $N_i^{-1} \mathfrak{S}_a N_i$ ungeändert. Da $\mathfrak{N}$ Normalisator von $\mathfrak{S}_a$ ist, also $\mathfrak{N}$ die Gruppe $\mathfrak{S}_a$ zur invarianten Untergruppe besitzt, hat man $N_i^{-1} \mathfrak{S}_a N_i = \mathfrak{S}_a$. Jede der Funktionen $(\sigma_1) \mathfrak{S}_a N_i, (\sigma_2) \mathfrak{S}_a N_i, \dots, (\sigma_l) \mathfrak{S}_a N_i$ ist mithin (vgl. Satz 4 des § 3, I Seite 24) eine rationale Funktion der voraussetzungsgemäß zu der Gruppe $\mathfrak{S}_a$ zugehörigen Größen $\sigma_1, \sigma_2, \dots, \sigma_l$. Hiermit ist die Existenz des Gleichungssystems (4) erwiesen und gezeigt, daß Σ das automorphe Untersystem Σ_a :

$$\left(\begin{smallmatrix} \sigma_1 \\ (\sigma_1) \end{smallmatrix} \mathfrak{S}_a N_i \begin{smallmatrix} \sigma_2 \\ (\sigma_2) \end{smallmatrix} \mathfrak{S}_a N_i \dots \begin{smallmatrix} \sigma_l \\ (\sigma_l) \end{smallmatrix} \mathfrak{S}_a N_i \right) \quad (i = 1, 2, \dots, n)$$

enthält, das der ersten Zeile von (3) entspricht. Sind N_i und N_k zwei Transmutationen aus $\mathfrak{N}$, so ist das Produkt der ihnen zugeordneten Transmutationen aus Σ_a , nämlich

$$\begin{aligned} & \left(\begin{smallmatrix} \sigma_1 \\ (\sigma_1) \end{smallmatrix} \mathfrak{S}_a N_i \begin{smallmatrix} \sigma_2 \\ (\sigma_2) \end{smallmatrix} \mathfrak{S}_a N_i \dots \begin{smallmatrix} \sigma_l \\ (\sigma_l) \end{smallmatrix} \mathfrak{S}_a N_i \right) \cdot \\ & \cdot \left(\begin{smallmatrix} \sigma_1 \\ (\sigma_1) \end{smallmatrix} \mathfrak{S}_a N_k \begin{smallmatrix} \sigma_2 \\ (\sigma_2) \end{smallmatrix} \mathfrak{S}_a N_k \dots \begin{smallmatrix} \sigma_l \\ (\sigma_l) \end{smallmatrix} \mathfrak{S}_a N_k \right) \\ & = \left(\begin{smallmatrix} \sigma_1 \\ (\sigma_1) \end{smallmatrix} \mathfrak{S}_a N_i \begin{smallmatrix} \sigma_2 \\ (\sigma_2) \end{smallmatrix} \mathfrak{S}_a N_i \dots \begin{smallmatrix} \sigma_l \\ (\sigma_l) \end{smallmatrix} \mathfrak{S}_a N_i \right) \cdot \\ & \cdot \left(\begin{smallmatrix} \sigma_1 \\ (\sigma_1) \end{smallmatrix} \mathfrak{S}_a N_i \begin{smallmatrix} \sigma_2 \\ (\sigma_2) \end{smallmatrix} \mathfrak{S}_a N_i \dots \begin{smallmatrix} \sigma_l \\ (\sigma_l) \end{smallmatrix} \mathfrak{S}_a N_i \right) \end{aligned}$$

$$= \left(\begin{matrix} \sigma_1 \\ (\sigma_1) \end{matrix} \mathfrak{S}_a N_i N_k \begin{matrix} \sigma_2 \\ (\sigma_2) \end{matrix} \mathfrak{S}_a N_i N_k \cdots \begin{matrix} \sigma_l \\ (\sigma_l) \end{matrix} \mathfrak{S}_a N_i N_k \right).$$

ersichtlich dem Produkt $\mathfrak{S}_a N_i \cdot \mathfrak{S}_a N_k$ zugeordnet. Das automorphe System Σ_a ist daher der Quotientengruppe $\mathfrak{N} \mathfrak{S}_a$ isomorph. Hiermit sind alle wesentlichen Aussagen des Satzes 1 bewiesen.

Da $\sigma_1, \sigma_2, \dots, \sigma_l$ nur rationale Funktionen der Dirigenten $\varrho_1, \varrho_2, \dots, \varrho_k$ des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ sind und $\mathfrak{S}_a N_i$ ebenfalls bloß automorphe Transmutationen der Größen $\varrho_1, \varrho_2, \dots, \varrho_k$ bedeuten, hat man im Gleichungssystem (4) ausschließlich Relationen zwischen $\varrho_1, \varrho_2, \dots, \varrho_k$ mit Koeffizienten aus P vor sich und kann hierauf jede Transmutation P_j ($j = 1, 2, \dots, p$) aus dem Transmutationssystem $\mathfrak{S}$ anwenden. Hierdurch erhält man:

$$(5) \quad \begin{cases} (\sigma_1) \mathfrak{S}_a N_i P_j = R_{1i}((\sigma_1) P_j, (\sigma_2) P_j, \dots, (\sigma_l) P_j) \\ (\sigma_2) \mathfrak{S}_a N_i P_j = R_{2i}((\sigma_1) P_j, (\sigma_2) P_j, \dots, (\sigma_l) P_j), \\ \vdots \\ (\sigma_l) \mathfrak{S}_a N_i P_j = R_{li}((\sigma_1) P_j, (\sigma_2) P_j, \dots, (\sigma_l) P_j), \end{cases}$$

($i = 1, 2, \dots, n; j = 1, 2, \dots, p$), wobei $P_1 = N_1 = \begin{pmatrix} \varrho_1 \varrho_2 \cdots \varrho_k \\ \varrho_1 \varrho_2 \cdots \varrho_k \end{pmatrix}$, also die identische Transmutation P_1 von $\mathfrak{S}$ bedeutet.

Wir behaupten: Ist P_j eine automorphe Transmutation aus $\mathfrak{S}$, befindet sich also P_j in der maximalen automorphen Untergruppe $\mathfrak{S}_a^{(m)}$ von $\mathfrak{S}$, und wird weiter vorausgesetzt, daß die unter (5) betrachteten Funktionen $(\sigma_1) \mathfrak{S}_a N_i P_j, (\sigma_2) \mathfrak{S}_a N_i P_j, \dots, (\sigma_l) \mathfrak{S}_a N_i P_j$ im Körper $(P; \sigma_1, \sigma_2, \dots, \sigma_l)$ gelegen sind, so gehört P_j dem Normalisator $\mathfrak{N}$ von $\mathfrak{S}_a$ an. Besteht nämlich für eine automorphe Transmutation P_j von $\mathfrak{S}$ das Gleichungssystem

$$(6) \quad \begin{cases} (\sigma_1) \mathfrak{S}_a N_i P_j = \lambda_1(\sigma_1, \sigma_2, \dots, \sigma_l), \\ (\sigma_2) \mathfrak{S}_a N_i P_j = \lambda_2(\sigma_1, \sigma_2, \dots, \sigma_l), \\ \vdots \\ (\sigma_l) \mathfrak{S}_a N_i P_j = \lambda_l(\sigma_1, \sigma_2, \dots, \sigma_l), \end{cases}$$

wobei die λ rationale Funktionen ihrer Argumente $\sigma_1, \sigma_2, \dots, \sigma_l$ mit Koeffizienten aus P bedeuten, so kann man auf (6), da es sich um Gleichungen zwischen $\varrho_1, \varrho_2, \dots, \varrho_k$ mit Koeffizienten aus P handelt, die Transmutationen $\mathfrak{S}_a$ aus $\mathfrak{S}$ anwenden; hierdurch ändert sich die rechte Seite von (6) überhaupt nicht, da die Funktionen $\sigma_1, \sigma_2, \dots, \sigma_l$ bei $\mathfrak{S}_a$ ihren Wert beibehalten. Mithin hat man:

$$\begin{aligned} (\sigma_1) \mathfrak{S}_a N_i P_j \mathfrak{S}_a &= (\sigma_1) \mathfrak{S}_a N_i P_j, (\sigma_2) \mathfrak{S}_a N_i P_j \mathfrak{S}_a = (\sigma_2) \mathfrak{S}_a N_i P_j, \dots, \\ (\sigma_l) \mathfrak{S}_a N_i P_j \mathfrak{S}_a &= (\sigma_l) \mathfrak{S}_a N_i P_j \text{ oder wegen (5):} \end{aligned}$$

$$(7) \quad \begin{cases} (\sigma_1) \mathfrak{S}_a N_i P_j \mathfrak{S}_a = R_{1i}((\sigma_1) P_j, (\sigma_2) P_j, \dots, (\sigma_l) P_j), \\ (\sigma_2) \mathfrak{S}_a N_i P_j \mathfrak{S}_a = R_{2i}((\sigma_1) P_j, (\sigma_2) P_j, \dots, (\sigma_l) P_j), \\ \vdots \\ (\sigma_l) \mathfrak{S}_a N_i P_j \mathfrak{S}_a = R_{li}((\sigma_1) P_j, (\sigma_2) P_j, \dots, (\sigma_l) P_j). \end{cases}$$

Auf das Gleichungssystem (7), das auch nur Relationen zwischen $q_1, q_2, \dots, q_k$ mit Koeffizienten aus P enthält, führe man die Transmutation P_j^{-1} aus, die wegen der Gruppeneigenschaft von $\mathfrak{S}_a^{(m)}$ zu $\mathfrak{S}$ gehört; dann erhält man unter Beachtung von (4):

$$(8) \quad \begin{cases} (\sigma_1) \mathfrak{S}_a N_i P_j \mathfrak{S}_a P_j^{-1} = (\sigma_1) \mathfrak{S}_a N_i, \\ (\sigma_2) \mathfrak{S}_a N_i P_j \mathfrak{S}_a P_j^{-1} = (\sigma_2) \mathfrak{S}_a N_i, \\ \vdots \\ (\sigma_l) \mathfrak{S}_a N_i P_j \mathfrak{S}_a P_j^{-1} = (\sigma_l) \mathfrak{S}_a N_i. \end{cases}$$

Auch die Gleichungen (8) lassen sich als Gleichungen zwischen $q_1, q_2, \dots, q_k$ mit Koeffizienten aus P auffassen und gestatten daher die Transmutation N_i^{-1} , die wegen des Gruppencharakters von $\mathfrak{N}$ zu $\mathfrak{S}$ gehört. Beachtet man noch, daß $\sigma_1, \sigma_2, \dots, \sigma_l$ durch $\mathfrak{S}_a$ ungeändert bleiben, so erhält man aus (8):

$$\begin{aligned} (\sigma_1) N_i P_j \mathfrak{S}_a P_j^{-1} N_i^{-1} &= \sigma_1, (\sigma_2) N_i P_j \mathfrak{S}_a P_j^{-1} N_i^{-1} = \sigma_2, \dots, \\ (\sigma_l) N_i P_j \mathfrak{S}_a P_j^{-1} N_i^{-1} &= \sigma_l. \end{aligned}$$

Da aber die l Funktionen $\sigma_1, \sigma_2, \dots, \sigma_l$ zu $\mathfrak{S}_a$ gehören, also bloß bei den Transmutationen $\mathfrak{S}_a$ von $\mathfrak{S}$ ihren Wert nicht verändern, muß $N_i P_j \mathfrak{S}_a P_j^{-1} N_i^{-1} = \mathfrak{S}_a$ sein, d. h. $N_i P_j$ ist mit $\mathfrak{S}_a$ vertauschbar, gehört also dem Normalisator $\mathfrak{N}$ an; folglich trifft dies auch für P_j als Produkt der zwei Elemente N_i^{-1} und $N_i P_j$ aus $\mathfrak{N}$ zu. Hieraus schließen wir: Außer den Transmutationen von Σ_a kann es in dem

Transmutationssystem Σ : $\left(\begin{smallmatrix} \sigma_1 \\ (\sigma_1) \mathfrak{S}_a N_i P_j \end{smallmatrix} \begin{smallmatrix} \sigma_2 \\ (\sigma_2) \mathfrak{S}_a N_i P_j \end{smallmatrix} \dots \begin{smallmatrix} \sigma_l \\ (\sigma_l) \mathfrak{S}_a N_i P_j \end{smallmatrix} \right)$ nur noch automorphe Transmutationen geben, wenn die P_j nicht in der maximalen automorphen Untergruppe $\mathfrak{S}_a^{(m)}$ von $\mathfrak{S}$ gelegen sind. Gibt es aber in Σ keine weiteren automorphen Transmutationen als die in Σ_a befindlichen, so ist Σ_a als maximale automorphe Untergruppe von Σ dessen Kern und $\mathfrak{N}|\mathfrak{S}_a$ ist isomorph zu dem Kern von Σ , das heißt Σ und $\|\mathfrak{S}|\mathfrak{S}_a\|$ sind isomorph, nicht hyperisomorph. Wir formulieren demnach als Ergänzung zu Satz 1 den

Satz 1_a. Ist für die Transmutationen P_j , die nicht der maximalen automorphen Untergruppe $\mathfrak{S}_a^{(m)}$ von $\mathfrak{S}$ angehören, keine der aus ihnen hergeleiteten Transmutationen

$$\left(\begin{smallmatrix} \sigma_1 \\ (\sigma_1) \end{smallmatrix} \mathfrak{S}_a N_i P_j \begin{smallmatrix} \sigma_2 \\ (\sigma_2) \end{smallmatrix} \mathfrak{S}_a N_i P_j \dots \begin{smallmatrix} \sigma_l \\ (\sigma_l) \end{smallmatrix} \mathfrak{S}_a N_i P_j \right)$$

eine automorphe Transmutation der Dirigenten $\sigma_1, \sigma_2, \dots, \sigma_l$ des Körpers $(P; \sigma_1, \sigma_2, \dots, \sigma_l)$, so sind Σ und $\|\mathfrak{S}|\mathfrak{S}_a\|$ isomorph.

Der im letzten Satz besprochene Fall tritt im besondern ein, wenn $\mathfrak{S}_a$ die identische Transmutation $E_1 = \begin{pmatrix} \varrho_1 & \varrho_2 & \dots & \varrho_k \\ \varrho_1 & \varrho_2 & \dots & \varrho_k \end{pmatrix}$ wird. Adjungiert man $\sigma_1, \sigma_2, \dots, \sigma_l$ zu dem Körper P , so reduziert sich alsdann das Transmutationssystem $\mathfrak{S}$ der Dirigenten $\varrho_1, \varrho_2, \dots, \varrho_k$ auf diejenigen seiner Transmutationen, die alle Funktionen $\sigma_1, \sigma_2, \dots, \sigma_l$ nicht ändern (Satz 4 des § 3, I Seite 24), also bei unserer Voraussetzung auf E_1 . Da E_1 die identische Transmutation ist, gehören demnach auch die Größen $\varrho_1, \varrho_2, \dots, \varrho_k$ dem Körper $(P; \sigma_1, \sigma_2, \dots, \sigma_l)$ an, und man hat Gleichungen

$$\varrho_h = \mu_h(\sigma_1, \sigma_2, \dots, \sigma_l) \quad (h = 1, 2, \dots, k),$$

wobei die auf der rechten Seite stehenden Größen rationale Funktionen ihrer Argumente bedeuten. Wendet man auf das letzte Gleichungssystem die Transmutation $N_i P_j$ an, die $\begin{pmatrix} \varrho_1 & \varrho_2 & \dots & \varrho_k \\ \varrho_{1j} & \varrho_{2j} & \dots & \varrho_{kj} \end{pmatrix}$ lauten möge, so erhält man

$$(9) \quad \varrho_{hj} = \mu_h((\sigma_1) N_i P_j, (\sigma_2) N_i P_j, \dots, (\sigma_l) N_i P_j) \quad (h = 1, 2, \dots, k).$$

Werden nunmehr $(\sigma_1) N_i P_j, (\sigma_2) N_i P_j, \dots, (\sigma_l) N_i P_j$ als Funktionen des Körpers $(P; \sigma_1, \sigma_2, \dots, \sigma_l)$ vorausgesetzt, so sind sie wegen der Zugehörigkeit von $\sigma_1, \sigma_2, \dots, \sigma_l$ zum Körper $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ auch solche des letzten Körpers. Als dann liegen wegen der Gleichungen (9) die Größen ϱ_{hj} ($h = 1, 2, \dots, k$) ebenfalls im Körper $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$, das heißt $N_i P_j$ ist eine automorphe Transmutation aus $\mathfrak{S}$. Mithin folgt aus Satz 1_a der

Satz 2. Ist $\mathfrak{S}$ das Transmutationssystem der Dirigenten $\varrho_1, \varrho_2, \dots, \varrho_k$ des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ und wählt man statt $\varrho_1, \varrho_2, \dots, \varrho_k$ irgendein andres Funktionensystem $\sigma_1, \sigma_2, \dots, \sigma_l$, das denselben Körper $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ erzeugt¹⁾, so ist das

¹⁾ Anders ausgedrückt: $\sigma_1, \sigma_2, \dots, \sigma_l$ soll ein zu E_1 zugehöriges Funktionensystem sein. Als dann kann man statt einer endlichen Anzahl $\sigma_1, \sigma_2, \dots, \sigma_l$ rationaler Funktionen von $\varrho_1, \varrho_2, \dots, \varrho_k$ auch die Gesamtheit aller im Körper $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ befindlichen rationalen Funktionen von $\varrho_1, \varrho_2, \dots, \varrho_k$ mit Koeffizienten aus P als zu E_1 zugehöriges System verwenden. Die Behandlung dieser unendlichen Funktionenmenge ist der Ausgangspunkt von R. DEDEKIND in den Supplementen zu P. G. LEJEUNE DIRICHLETS Vorlesungen über Zahlentheorie, 4. Auflage, Braunschweig 1894, S. 456ff. bei seinem Studium der Abbildungen

Transmutationssystem Σ der Dirigenten $\sigma_1, \sigma_2, \dots, \sigma_l$ des mit $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ übereinstimmenden Körpers $(P; \sigma_1, \sigma_2, \dots, \sigma_l)$ isomorph zu $\mathfrak{S}$.

Das Transmutationssystem eines Körpers ist also, wenn isomorphe Transmutationssysteme als nicht verschieden gelten, unabhängig von der Wahl eines den Körper erzeugenden Dirigentensystems.

Wir spezialisieren den letzten Satz für den Fall $l=1$, wählen also eine primitive Funktion $\sigma_e(\varrho_1, \varrho_2, \dots, \varrho_k)$. Alsdann wird das Transmutationssystem Σ der Dirigente σ_e des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ von der Form $\begin{pmatrix} \sigma_e \\ \sigma_{ei} \end{pmatrix}$, wobei σ_{ei} alle Wurzeln der irreduziblen Gleichung $N(x)=0$ mit Koeffizienten aus P durchläuft, die durch σ_e befriedigt wird. Für die identische Transmutation $E_1 = \begin{pmatrix} \varrho_1 & \varrho_2 & \dots & \varrho_k \\ \varrho_1 & \varrho_2 & \dots & \varrho_k \end{pmatrix}$ ist der Normalisator $\mathfrak{N}$ die maximale automorphe Untergruppe $\mathfrak{S}_a^{(m)}$ von $\mathfrak{S}$. Infolge des Isomorphismus von $\mathfrak{S}$ und Σ ergibt sich demnach aus Satz 1 und 2 der

Satz 3. $\mathfrak{S}$ sei das Transmutationssystem der Dirigenten $\varrho_1, \varrho_2, \dots, \varrho_k$ des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ und besitze die maximale automorphe Untergruppe $\mathfrak{S}_a^{(m)}$, die aus den n Transmutationen $E_1, N_2, N_3, \dots, N_n$ bestehe, also $\mathfrak{S}_a^{(m)} = E_1 + N_2 + N_3 + \dots + N_n$. Die GALOISSCHE Zerlegung von $\mathfrak{S}$ nach $\mathfrak{S}_a^{(m)}$ laute:

$$\mathfrak{S} = \mathfrak{S}_a^{(m)} + \mathfrak{S}_a^{(m)} P_2 + \mathfrak{S}_a^{(m)} P_3 + \dots + \mathfrak{S}_a^{(m)} P_p.$$

Jede primitive Funktion $\sigma_e(\varrho_1, \varrho_2, \dots, \varrho_k)$ des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ genügt dann einer irreduziblen Gleichung $N(x)=0$ des Grades np mit Koeffizienten aus P , und die Wurzeln dieser Gleichung zerfallen in p Gruppen von je n Größen¹⁾:

eines Körpers. Auf die knapp gehaltenen Untersuchungen dieses großen Mathematikers, die er bereits 1857–1858 in Göttingen vorgetragen hat (vgl. a. a. O. S. 484) und die H. WEBER (vgl. Lehrbuch der Algebra, 2. Aufl., 1. Bd., S. VII, Braunschweig 1898) kannte, ohne daß sie auf die Literatur Einfluß gehabt zu haben scheinen, bin ich erst nachträglich aufmerksam geworden. DEDEKINDS Resultate berühren sich, wenn man sie aus seiner Sprache und Auffassung überträgt, vielfach mit den meinigen in § 1 und 2; die Ableitung ist eine verschiedenartige.

¹⁾ Dies ist die Spezialisierung der Gleichungen (4) und (5) für den Fall $l=1$. Die Einteilung der Wurzeln einer irreduziblen Gleichung in Gruppen geht auf N. H. ABELS Arbeit „Sur une classe particulière d'équations résolubles

$$(9) \begin{cases} (\sigma_e) (Q_1, Q_2, \dots, Q_k), (\sigma_e) N_2 = R_2(\sigma_e), \dots, (\sigma_e) N_n = R_n(\sigma_e), \\ (\sigma_e) P_2, (\sigma_e) N_2 P_2 = R_2((\sigma_e) P_2), \dots, (\sigma_e) N_n P_2 = R_n((\sigma_e) P_2), \\ \vdots \\ (\sigma_e) P_p, (\sigma_e) N_2 P_p = R_2((\sigma_e) P_p), \dots, (\sigma_e) N_n P_p = R_n((\sigma_e) P_p), \end{cases}$$

wobei die Größen R rationale Funktionen ihrer Argumente sind. Keine in der zweiten bis p -ten Zeile stehende Wurzel ist rational durch σ_e ausdrückbar. Kürzer: Das Transmutationssystem $\left(\begin{smallmatrix} \sigma_e \\ (\sigma_e) N_i P_j \end{smallmatrix} \right)$ ($i = 1, 2, \dots, n; j = 1, 2, \dots, p$) ist zu $\mathfrak{S}$ isomorph.

Man kann den Satz 3 noch dahin ergänzen: **Jede Wurzel** einer Zeile des Schemas (9) ist rationale Funktion einer jeden beliebigen Wurzel, die sich in der gleichen Zeile befindet; hingegen ist niemals eine Wurzel einer Zeile des Schemas (9) rationale Funktion einer Wurzel, die sich in einer anderen Zeile befindet.

Bedeutet N_a irgendeine feste Transmutation aus der maximalen automorphen Untergruppe $\mathfrak{S}_a^{(m)}$ von $\mathfrak{S}$, so erhält man durch ihre Anwendung auf die Gleichungen der ersten Zeile von (9):

$$(10) \quad (\sigma_e) N_a, (\sigma_e) N_2 N_a = R_2((\sigma_e) N_a), (\sigma_e) N_3 N_a = R_3((\sigma_e) N_a), \dots, \\ (\sigma_e) N_n N_a = R_n((\sigma_e) N_a).$$

Da die letzten Gleichungen auch nur Relationen zwischen $Q_1, Q_2, \dots, Q_k$ mit Koeffizienten aus P sind, kann man auf sie die Transmutationen $P_2, P_3, \dots, P_p$ aus $\mathfrak{S}$ anwenden: hierdurch ergibt sich als Fortsetzung von (10)

$$(10) \begin{cases} (\sigma_e) N_a P_2, (\sigma_e) N_2 N_a P_2 = R_2((\sigma_e) N_a P_2), (\sigma_e) N_3 N_a P_2 = \\ \quad = R_3((\sigma_e) N_a P_2), \dots, (\sigma_e) N_n N_a P_2 = R_n((\sigma_e) N_a P_2), \\ \vdots \\ (\sigma_e) N_a P_p, (\sigma_e) N_2 N_a P_p = R_2((\sigma_e) N_a P_p), (\sigma_e) N_3 N_a P_p \\ \quad = R_3((\sigma_e) N_a P_p), \dots, (\sigma_e) N_n N_a P_p = R_n((\sigma_e) N_a P_p). \end{cases}$$

Nun sind $N_a, N_2 N_a, N_3 N_a, \dots, N_n N_a$, abgesehen von der Reihenfolge, ebenfalls alle Elemente $E_1, N_2, N_3, \dots, N_n$ von $\mathfrak{S}_a^{(m)}$. Mithin

algébriquement^a, Journ. f. r. u. ang. Math. 4 (1829), § 1 zurück. Unsere Zerlegung (9) ist eine Zusammenfassung der in Abels Schema auftretenden Gruppen von Wurzeln, so daß sich in einer Zeile nicht wie bei Abel iterierte, sondern nur rationale Funktionen einer Wurzel aus der Zeile befinden. Abel zerlegt nämlich, wie man seinen Prozeß beschreiben kann, nicht nach $\mathfrak{S}_a^{(m)}$, sondern nach irgendeiner Untergruppe von $\mathfrak{S}_a^{(m)}$, die aus einer Transmutation und ihren Potenzen besteht.

haben wir in (10) genau dieselben Größen wie im System (9) vor uns; nur haben die in der nämlichen Zeile stehenden Elemente, die jetzt als rationale Funktionen irgendeiner Wurzel $(\sigma_e)N_a, (\sigma_e)N_aP_2, \dots, (\sigma_e)N_aP_p$ der Zeile dargestellt sind, eventuell ihre Reihenfolge vertauscht.

Um noch zu zeigen, daß niemals eine Wurzel irgendeiner Zeile des Schemas (9) oder (10) rationale Funktion einer Wurzel aus einer anderen Zeile sein kann, braucht man nur zu beachten, daß $(\sigma_e)N_aP_i$, wenn $P_i = \begin{pmatrix} \varrho_1 & \varrho_2 & \dots & \varrho_k \\ \varrho_{1i} & \varrho_{2i} & \dots & \varrho_{ki} \end{pmatrix}$ ist, für den Körper $(P; \varrho_{1i}, \varrho_{2i}, \dots, \varrho_{ki})$ die gleiche Rolle als primitive Funktion wie $\sigma_e(\varrho_1, \varrho_2, \dots, \varrho_k)$ für den Körper $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ spielt. Maximale automorphe Untergruppe von $P_i^{-1}\mathfrak{S}$ ist $P_i^{-1}\mathfrak{S}_a^{(m)}P_i$, wofür man wegen der Zugehörigkeit von N_a zur Gruppe $\mathfrak{S}_a^{(m)}$ auch $P_i^{-1}N_a^{-1}\mathfrak{S}_a^{(m)}N_aP_i$ schreiben kann. Die Elemente dieser Gruppe erzeugen aus $(\sigma_e)N_aP_i$ die Wurzeln der i -ten Zeile von (10), nämlich

$$\begin{aligned} & (\sigma_e)N_aP_i, (\sigma_e)N_aP_i(P_i^{-1}N_a^{-1}N_2N_aP_i) = \\ & = (\sigma_e)N_2N_aP_i, \dots, (\sigma_e)N_aP_i(P_i^{-1}N_a^{-1}N_nN_aP_i) = (\sigma_e)N_nN_aP_i. \end{aligned}$$

Für den Körper $(P; \varrho_{1i}, \varrho_{2i}, \dots, \varrho_{ki})$ wird die i -te Zeile des Schemas (10) zur ersten, und wie sich im ursprünglichen Schema (10) keine Wurzel, die nicht in der ersten Zeile steht, durch das erste Element $(\sigma_e)N_a$ ausdrücken läßt, kann auch keine Wurzel durch $(\sigma_e)N_aP_i$ rational ausgedrückt werden; es sei denn, daß sie mit $(\sigma_e)N_aP_i$ in gleicher Zeile steht.

Hat man irgendeine irreduzible Gleichung $N(x)=0$ mit Koeffizienten aus P und der Wurzel σ_e , so bestimmt für sie das Transmutationssystem der Dirigente σ_e des Körpers $(P; \sigma_e)$ oder das Verteilungsschema (9) der Wurzeln eine Zahl p , die man die Faltigkeit der irreduziblen Gleichung nennen könnte. Die Zahl $p = \frac{np}{n}$ ist der Index oder der Quotient aus der Anzahl der Transmutationen durch die Anzahl der automorphen Transmutationen oder gleich der Anzahl der nicht identischen, durch die Gleichungswurzeln definierten Körper. Im Falle $p=1$, wo die Wurzeln der Gleichung nur einen einzigen Körper definieren, bezeichnet man die Gleichung als Normalgleichung oder GALOISsche Gleichung.¹⁾

¹⁾ Vgl. § 2 (I, S. 17).

§ 6.

Der Galoissche Körper und sein Transmutationssystem. Der Galoissche Oberkörper $\mathfrak{K}$ eines Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ und die Darstellung des Transmutationssystems der Dirigenten $\varrho_1, \varrho_2, \dots, \varrho_k$ des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ in $\mathfrak{K}$.

Ein Körper $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ heißt ein GALOISScher oder Normalkörper, wenn das Transmutationssystem $\mathfrak{S}$ seiner Dirigenten nur automorphe Transmutationen besitzt, also $\mathfrak{S}$ mit seiner maximalen automorphen Untergruppe $\mathfrak{S}_a^{(m)}$ zusammenfällt.

Wir beweisen den

Satz 1. Ist $\mathfrak{S}$ das Transmutationssystem irgendeines Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$, $\mathfrak{S}_a^{(m)}$ die maximale automorphe Untergruppe von $\mathfrak{S}$, und bedeuten $\sigma_1(\varrho_1, \varrho_2, \dots, \varrho_k)$, $\sigma_2(\varrho_1, \varrho_2, \dots, \varrho_k)$, $\dots$, $\sigma_l(\varrho_1, \varrho_2, \dots, \varrho_k)$ beliebige rationale Funktionen von $\varrho_1, \varrho_2, \dots, \varrho_k$ mit Koeffizienten aus P , so bilden die in $\mathfrak{S}_a^{(m)}$ enthaltenen Transmutationen, die sämtliche l Funktionen $\sigma_1, \sigma_2, \dots, \sigma_l$ nicht ändern, eine Gruppe.

In der Tat seien A und B zwei Transmutationen aus $\mathfrak{S}_a^{(m)}$, die beide $\sigma_1, \sigma_2, \dots, \sigma_l$ ihrem Werte nach nicht ändern, für die also $(\sigma_1)A = \sigma_1$, $(\sigma_2)A = \sigma_2, \dots, (\sigma_l)A = \sigma_l$ und $(\sigma_1)B = \sigma_1$, $(\sigma_2)B = \sigma_2, \dots, (\sigma_l)B = \sigma_l$ ist. Da A eine automorphe Transmutation aus $\mathfrak{S}$ ist, hat man in $(\sigma_1)A = \sigma_1$, $(\sigma_2)A = \sigma_2, \dots, (\sigma_l)A = \sigma_l$ auch nur Gleichungen zwischen $\varrho_1, \varrho_2, \dots, \varrho_k$ mit Koeffizienten aus P vor sich und kann demnach auf sie die Transmutation B aus $\mathfrak{S}$ anwenden. Hierdurch erhält man $(\sigma_1)AB = (\sigma_1)B$, $(\sigma_2)AB = (\sigma_2)B, \dots, (\sigma_l)AB = (\sigma_l)B$ oder bei Beachtung des oben angegebenen zweiten Gleichungssystems $(\sigma_1)AB = \sigma_1$, $(\sigma_2)AB = \sigma_2, \dots, (\sigma_l)AB = \sigma_l$, d. h. auch das Produkt AB der zwei automorphen Transmutationen A und B von $\mathfrak{S}_a^{(m)}$ ändert alle Funktionen $\sigma_1, \sigma_2, \dots, \sigma_l$ nicht. Diese Abgeschlossenheit in bezug auf die Produktbildung der in der endlichen Gruppe $\mathfrak{S}_a^{(m)}$ enthaltenen Transmutationen, die alle Funktionen $\sigma_1, \sigma_2, \dots, \sigma_l$ nicht ändern, ist aber ausreichend dafür, daß diese Transmutationen eine Gruppe bilden.

Da für einen GALOISSchen Körper keine außerhalb $\mathfrak{S}_a^{(m)}$ befindlichen Transmutationen von $\mathfrak{S}$ existieren, ergibt sich aus Satz 1 der

Satz 2. Ist $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ ein GALOISScher Körper, so existiert zu jedem System $\sigma_1(\varrho_1, \varrho_2, \dots, \varrho_k)$, $\sigma_2(\varrho_1, \varrho_2, \dots, \varrho_k), \dots, \sigma_l(\varrho_1, \varrho_2, \dots, \varrho_k)$ rationaler Funktionen von $\varrho_1, \varrho_2, \dots, \varrho_k$ mit Koeffizienten aus P eine Gruppe $\mathfrak{S}_a$ von Transmutationen, so daß sich jede der Funktionen $\sigma_1, \sigma_2, \dots, \sigma_l$ bei allen $\mathfrak{S}_a$ angehörigen Transmutationen nicht ändert, hingegen min-

destens eine von ihnen bei jeder $\mathfrak{S}_a$ nicht angehörigen Transmutation von $\mathfrak{S}$ einen anderen Wert annimmt. Bei einem GALOISSchen Körper gehört also nicht nur wie bei jedem Körper zu jeder automorphen Untergruppe $\mathfrak{S}_a$ ein System rationaler Funktionen $\sigma_1(\varrho_1, \varrho_2, \dots, \varrho_k), \sigma_2(\varrho_1, \varrho_2, \dots, \varrho_k), \dots, \sigma_l(\varrho_1, \varrho_2, \dots, \varrho_k)$, sondern auch umgekehrt definiert hier jedes beliebige System rationaler Funktionen $\sigma_1(\varrho_1, \varrho_2, \dots, \varrho_k), \sigma_2(\varrho_1, \varrho_2, \dots, \varrho_k), \dots, \sigma_l(\varrho_1, \varrho_2, \dots, \varrho_k)$ eine zugehörige automorphe Untergruppe $\mathfrak{S}_a$.

Für den GALOISSchen Körper folgt weiter aus dem Satz 1a des § 5, da es bei dem GALOISSchen Körper keine Transmutationen gibt, die nicht $\mathfrak{S}_a^{(m)}$ angehören, der

Satz 3. Ist $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ ein GALOISScher Körper und bedeuten $\sigma_1(\varrho_1, \varrho_2, \dots, \varrho_k), \sigma_2(\varrho_1, \varrho_2, \dots, \varrho_k), \dots, \sigma_l(\varrho_1, \varrho_2, \dots, \varrho_k)$ rationale Funktionen von $\varrho_1, \varrho_2, \dots, \varrho_k$ mit Koeffizienten aus P , die bei der automorphen Untergruppe $\mathfrak{S}_a$ des Transmutationssystem $\mathfrak{S}$ der Dirigenten $\varrho_1, \varrho_2, \dots, \varrho_k$ ihren Wert nicht ändern, so ist das Transmutationssystem Σ der Dirigenten $\sigma_1, \sigma_2, \dots, \sigma_l$ des Körpers $(P; \sigma_1, \sigma_2, \dots, \sigma_l)$ isomorph zu $\|\mathfrak{S}|\mathfrak{S}_a\|$.

Definition. Unter dem GALOISSchen Oberkörper eines Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ soll der kleinste aus P entstehende Körper verstanden werden, der unter seinen Dirigenten die Größen $\varrho_1, \varrho_2, \dots, \varrho_k$ enthält und nur automorphe Transmutationen zuläßt.

Hat man irgendeinen Körper $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$, so gibt es in dem Transmutationssystem $\mathfrak{S}$ der Dirigenten $\varrho_1, \varrho_2, \dots, \varrho_k$ Transmutationen, die ϱ_1 in jede Wurzel der irreduziblen Gleichung $X_1(x) = 0$ mit Koeffizienten aus P überführen, die durch ϱ_1 befriedigt wird. Aus der Gleichberechtigung von $\varrho_2, \varrho_3, \dots, \varrho_k$ mit ϱ_1 ergibt sich, daß es unter den Transmutationen von $\mathfrak{S}$ solche gibt, die ϱ_2 in alle Wurzeln der durch ϱ_2 befriedigten, irreduziblen Gleichung $X_1^{(2)}(x) = 0$ mit Koeffizienten aus P überführen usw.

Schließlich enthält $\mathfrak{S}$ Transmutationen, die ϱ_k in jede Wurzel der irreduziblen Gleichung mit Koeffizienten aus P überführen, die durch ϱ_k befriedigt wird und die wir mit $X_1^{(k)}(x) = 0$ bezeichnen. Hieraus folgt: In einem aus P hervorgehenden Körper, der unter seinen Dirigenten die Größen $\varrho_1, \varrho_2, \dots, \varrho_k$ enthält und nur automorphe, d. h. im Erweiterungskörper von P sich vollziehende Transmutationen besitzen soll, müssen notwendig alle Wurzeln der k in P irreduziblen Gleichungen $X_1(x) = 0, X_1^{(2)}(x) = 0, \dots, X_1^{(k)}(x) = 0$ gelegen sein, die durch $\varrho_1, \varrho_2, \dots, \varrho_k$

befriedigt werden. Man hat demnach die übliche Definition des GALOISSchen Oberkörpers eines Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$: Der GALOISSche Oberkörper $\mathfrak{K}$ des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ ist derjenige aus P hervorgehende kleinste Körper, in dem sich alle Wurzeln der Gleichung $K(x) = 0$ befinden; hierbei bedeutet $K(x)$ das kleinste gemeinsame Vielfache der ganzen Funktionen $X_1(x), X_1^{(2)}(x), \dots, X_1^{(k)}(x)$, und es sind $X_1(x) = 0, X_1^{(2)}(x) = 0, X_1^{(3)}(x) = 0, \dots, X_1^{(k)}(x) = 0$ die irreduziblen Gleichungen mit Koeffizienten aus P , die der Reihe nach durch die Größen $\varrho_1, \varrho_2, \dots, \varrho_k$ befriedigt werden.

Da sich im GALOISSchen Oberkörper von $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ alle Transmutationen der Dirigenten $\varrho_1, \varrho_2, \dots, \varrho_k$ vollziehen, kann man nach dem Satz 7 des § 4 (I S. 50) den GALOISSchen Oberkörper von $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ auch so definieren: Der GALOISSche Oberkörper eines Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ wird erzeugt durch eine primitive Funktion $\sigma_c(\varrho_1, \varrho_2, \dots, \varrho_k)$ der Größen $\varrho_1, \varrho_2, \dots, \varrho_k$ in Gemeinschaft mit den anderen Wurzeln der irreduziblen Gleichung mit Koeffizienten aus P , die durch σ_c befriedigt wird. Von diesen Gleichungswurzeln (vgl. die ergänzende Bemerkung oben auf S. 13 zu Satz 3 des § 5) sind zur Erzeugung des GALOISSchen Oberkörpers nur $\frac{s}{n}$ nicht durch einander rational ausdrückbare ausreichend; dabei ist s die Anzahl der Transmutationen $\mathfrak{S}$ der Dirigenten $\varrho_1, \varrho_2, \dots, \varrho_k$ des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ und n die in der maximalen automorphen Untergruppe $\mathfrak{S}_a^{(m)}$ von $\mathfrak{S}$ befindlichen.

Hieraus folgt als charakteristisches Kennzeichen für den GALOISSchen Körper ($n = s$), daß seine primitiven Funktionen GALOISSchen Gleichungen genügen.

Nach § 2 ist das Transmutationssystem aller Wurzeln einer Gleichung die GALOISSche Gruppe der Gleichung. Da man den GALOISSchen Oberkörper $\mathfrak{K}$ von dem Körper $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ auch durch Adjunktion aller Wurzeln der irreduziblen Gleichung mit Koeffizienten aus P erzeugen kann, die durch eine primitive Funktion $\sigma_c(\varrho_1, \varrho_2, \dots, \varrho_k)$ befriedigt wird, und weiter nach Satz 2 des § 5 die Transmutationssysteme aller möglichen einen Körper erzeugenden Dirigenten isomorph sind, ergibt sich für den Körper $\mathfrak{K}$ der

Satz 4. $\mathfrak{K}$ sei der GALOISSche Oberkörper des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ der Dirigenten $\varrho_1, \varrho_2, \dots, \varrho_k$. Weiter sei $\lambda_1, \lambda_2, \dots, \lambda_t$ irgendein System erzeugender Größen für den Körper $\mathfrak{K}$, und $\mathfrak{P}$ bedeute das Transmutationssystem der Diri-

genten $\lambda_1, \lambda_2, \dots, \lambda_t$ des mit $\mathfrak{K}$ übereinstimmenden Körpers $(P; \lambda_1, \lambda_2, \dots, \lambda_t)$. Dann ist $\mathfrak{P}$, weil $\mathfrak{K}$ ein GALOISScher Körper ist, eine Gruppe und isomorph mit dem Transmutationssystem eines jeden den Körper $\mathfrak{K}$ erzeugenden Systems von Dirigenten; im besondern ist $\mathfrak{P}$ isomorph mit der GALOISSchen Gruppe jeder in P irreduziblen Gleichung, die irgendeine primitive Funktion σ_e des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ zur Wurzel hat.

Wird der GALOISSche Oberkörper $\mathfrak{K}$ des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ durch Adjunktion der Größen $\lambda_1, \lambda_2, \dots, \lambda_t$ aus P erzeugt, so sind $\varrho_1, \varrho_2, \dots, \varrho_k$ als im Körper $\mathfrak{K}$ gelegene Größen rationale Funktionen von $\lambda_1, \lambda_2, \dots, \lambda_t$ mit Koeffizienten aus P . Da der Körper $(P; \lambda_1, \lambda_2, \dots, \lambda_t)$, das heißt der Körper $\mathfrak{K}$, ein GALOISScher Körper ist, läßt sich auf $\mathfrak{K}$ der Satz 3 dieses Paragraphen anwenden, und man erhält den wichtigen

Satz 5. Ist $\mathfrak{S}$ das Transmutationssystem der Dirigenten $\varrho_1, \varrho_2, \dots, \varrho_k$ des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ und bedeutet ferner $\mathfrak{P}$ das Transmutationssystem irgendwelcher Dirigenten $\lambda_1, \lambda_2, \dots, \lambda_t$, die den GALOISSchen Oberkörper $\mathfrak{K} \equiv (P; \lambda_1, \lambda_2, \dots, \lambda_t)$ von $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ erzeugen, so ist $\mathfrak{S}$ isomorph zu der Quotientenmischgruppe $\|\mathfrak{P} | \mathfrak{P}_{\varrho_1 \varrho_2 \dots \varrho_k}\|$; dabei ist $\mathfrak{P}_{\varrho_1 \varrho_2 \dots \varrho_k}$ diejenige Untergruppe von $\mathfrak{P}$, bei der jede der rationalen Funktionen $\varrho_1, \varrho_2, \dots, \varrho_k$ von $\lambda_1, \lambda_2, \dots, \lambda_t$ einzeln ungeändert bleibt.

Der Satz 5 beweist die Möglichkeit der isomorphen Darstellbarkeit eines Transmutationssystems $\mathfrak{S}$ durch eine Gruppe $\mathfrak{P}$ und eine ihrer Untergruppen $\mathfrak{P}_{\varrho_1 \varrho_2 \dots \varrho_k}$, so daß $\mathfrak{S}$ isomorph ist zu den Komplexen

$\mathfrak{P}_{\varrho_1 \varrho_2 \dots \varrho_k}, \mathfrak{P}_{\varrho_1 \varrho_2 \dots \varrho_k} P_2, \mathfrak{P}_{\varrho_1 \varrho_2 \dots \varrho_k} P_3, \dots, \mathfrak{P}_{\varrho_1 \varrho_2 \dots \varrho_k} P_s$,
die sich bei der GALOISSchen Zerlegung der Gruppe $\mathfrak{P}$ nach ihrer Untergruppe $\mathfrak{P}_{\varrho_1 \varrho_2 \dots \varrho_k}$ ergeben.

§ 7.

Die P-Transmutationssysteme, insbesondere die imprimitiven Systeme. Imprimitive Gleichungen und imprimitive Körper.

$$(1) \left\{ \begin{array}{l} a_1, a_2, \dots, a_t, \\ a_1^{(2)}, a_2^{(2)}, \dots, a_t^{(2)}, \\ \vdots \\ a_1^{(t)}, a_2^{(t)}, \dots, a_t^{(t)}, \end{array} \right.$$

seien t Systeme von je l Größen, die sämtlich voneinander verschieden sind. $\mathfrak{G}$ bedeute eine transitive Permutationsgruppe der Größen

$a_1, a_2, \dots, a_l$. Die Permutationen von G lauten $\begin{pmatrix} a_1 & a_2 & \dots & a_l \\ a_{\gamma_1} & a_{\gamma_2} & \dots & a_{\gamma_l} \end{pmatrix}$, wobei $a_{\gamma_1}, a_{\gamma_2}, \dots, a_{\gamma_l}$ bis auf die Reihenfolge mit $a_1, a_2, \dots, a_l$ übereinstimmen und $\mathfrak{G}$ entsprechend dem transitiven Charakter der Permutationsgruppe $\mathfrak{G}$ unter seinen Permutationen l enthält, die a_1 in a_1 beziehungsweise in $a_2, a_3, \dots, a_l$ überführen. Weiter sei

$$\Pi_i = \begin{pmatrix} a_1 & a_2 & \dots & a_l \\ a_1^{(i)} & a_2^{(i)} & \dots & a_l^{(i)} \end{pmatrix} \quad (i = 2, 3, \dots, t)$$

eine Transmutation von $a_1, a_2, \dots, a_l$ in $a_1^{(i)}, a_2^{(i)}, \dots, a_l^{(i)}$. Dann bilde man das System

$$\Sigma = \mathfrak{G} + \mathfrak{G}\Pi_2 + \mathfrak{G}\Pi_3 + \dots + \mathfrak{G}\Pi_t$$

Das System Σ mit den beschriebenen Eigenschaften soll ein P-Transmutationssystem der Dirigenten $a_1, a_2, \dots, a_l$ heißen. Das Wesentliche der P-Transmutationssysteme ist, daß sie t transitive Permutationsgruppen, nämlich $\mathfrak{G}$ mit den Permutationen $\begin{pmatrix} a_1 & a_2 & \dots & a_l \\ a_{\gamma_1} & a_{\gamma_2} & \dots & a_{\gamma_l} \end{pmatrix}$ und $\Pi_i^{-1}\mathfrak{G}\Pi_i$ mit den Permutationen $\begin{pmatrix} a_1^{(i)} & a_2^{(i)} & \dots & a_l^{(i)} \\ a_{\gamma_1}^{(i)} & a_{\gamma_2}^{(i)} & \dots & a_{\gamma_l}^{(i)} \end{pmatrix} \quad (i = 2, 3, \dots, t)$ liefern, die nur in anderen, aber stets verschiedenen Symbolen geschrieben sind.

Als imprimitive P-Transmutationssysteme oder kurz imprimitive Transmutationssysteme definieren wir solche, bei denen $1 < l < tl$, das heißt solche P-Transmutationssysteme, die eine von der identischen Permutation verschiedene transitive Permutationsgruppe $\mathfrak{G}$ enthalten und hierdurch nicht erschöpft werden. Diese imprimitiven Transmutationssysteme charakterisieren die imprimitiven Gleichungen und weiter die imprimitiven Körper. Wir geben folgende **Definition der imprimitiven Gleichungen**: Eine Gleichung $f(x) = 0$ vom Grade n mit Koeffizienten aus P heißt imprimitiv, wenn sie in P irreduzibel ist und durch Adjunktion aller Wurzeln $\vartheta_1, \vartheta_2, \dots, \vartheta_t$ einer in P irreduziblen Gleichung $\varphi(x) = 0$ vom Grade t , wobei $1 < t < n$ ist, in das Produkt

$$(2) \quad f(x) = c f_1(x; \vartheta_1) f_1(x; \vartheta_2) \dots f_1(x; \vartheta_t)$$

zerfällt, wobei c eine P angehörige Konstante und $f_1(x; \vartheta_i)$ eine ganze Funktion von x mit Koeffizienten aus dem Körper $(P; \vartheta_i)$ bedeutet.

Wegen der Irreduzibilität von $f(x) = 0$ kann für keine Wurzel a von $f(x) = 0$ gleichzeitig $f_1(a; \vartheta_i) = 0$ und $f_1(a; \vartheta_k) = 0$ sein, wobei ϑ_i und ϑ_k zwei verschiedene der Wurzeln von $\varphi(x) = 0$ bedeuten. Aus dem gleichzeitigen Bestehen der Gleichungen $f_1(a; \vartheta_i) = 0$ und $f_1(a; \vartheta_k) = 0$

würde nämlich im Widerspruch zu der vorausgesetzten Irreduzibilität von $f(x)=0$ aus der Zerlegung (2) folgen, daß α mindestens zweifache Wurzel von $f(x)=0$ ist. Durch die Zerlegung (2) zerfallen demnach die n Wurzeln von $f(x)=0$ in t Systeme:

$$(1) \begin{cases} \alpha_1^{(1)}, \alpha_2^{(1)}, \dots, \alpha_l^{(1)}, \\ \alpha_1^{(2)}, \alpha_2^{(2)}, \dots, \alpha_l^{(2)}, \\ \vdots \\ \alpha_1^{(t)}, \alpha_2^{(t)}, \dots, \alpha_l^{(t)}, \end{cases}$$

so daß $\alpha_1^{(i)}, \alpha_2^{(i)}, \dots, \alpha_l^{(i)}$ die Wurzeln von $f_1(x; \vartheta_i)=0$ bedeuten; dabei hat $f_1(x; \vartheta_i)$ wegen der Zerlegung (2) den Grad $l = \frac{n}{t}$. Da $f_1(\alpha_1^{(i)}; \vartheta_i)=0$ ist, hat die Gleichung $f_1(\alpha_1^{(i)}; x)=0$ die Wurzel ϑ_i , und ferner besitzt sie mit $\varphi(x)=0$ außer ϑ_i keine gemeinsame Wurzel, weil, wie schon oben hervorgehoben, sonst $f(x)=0$ als Folge der Zerlegung (2) die Größe $\alpha_1^{(i)}$ zur mindestens zweifachen Wurzel hätte. Mithin ist der größte gemeinsame Teiler von $\varphi(x)$ und $f_1(\alpha_1^{(i)}; x)$ die Linearfunktion $x-\vartheta_i$. Der größte gemeinsame Teiler zweier ganzer Funktionen läßt sich aber mit Hilfe des Euclidischen Algorithmus rational finden; daher besitzt ϑ_i einen Wert aus dem Körper der Koeffizienten von $\varphi(x)$ und $f_1(\alpha_1^{(i)}; x)$. Es existiert demnach eine rationale Funktion $R(\alpha_1^{(i)})$ mit Koeffizienten aus P , so daß $\vartheta_i = R(\alpha_1^{(i)})$ ($i=1, 2, \dots, t$) wird. Ebenso wie $\alpha_1^{(i)}$ haben auch die mit $\alpha_1^{(i)}$ in der gleichen Zeile stehenden Größen, $\alpha_2^{(i)}, \alpha_3^{(i)}, \dots, \alpha_l^{(i)}$ nach ihrer Wahl die Eigenschaft, daß $f_1(\alpha_2^{(i)}; \vartheta_i)=0$, $f_1(\alpha_3^{(i)}; \vartheta_i)=0, \dots, f_1(\alpha_l^{(i)}; \vartheta_i)=0$ ($i=1, 2, \dots, t$) ist. Folglich hat man:

$$\vartheta_i = R(\alpha_1^{(i)}) = R(\alpha_2^{(i)}) = \dots = R(\alpha_l^{(i)}) \quad (i=1, 2, \dots, t).$$

Hiermit ist das Resultat gewonnen: Bedeutet $f(x)=0$ eine imprimitive Gleichung, so lassen sich die Gleichungswurzeln von $f(x)=0$ nach dem Schema (1) einteilen, und es existiert eine rationale Funktion $R(x)$ mit Koeffizienten aus P , so daß die t Wurzeln von $\varphi(x)=0$ lauten:

$$\begin{aligned} \vartheta_1 &= R(\alpha_1^{(1)}) = R(\alpha_2^{(1)}) = \dots = R(\alpha_l^{(1)}), \\ \vartheta_2 &= R(\alpha_1^{(2)}) = R(\alpha_2^{(2)}) = \dots = R(\alpha_l^{(2)}), \\ &\vdots \\ \vartheta_t &= R(\alpha_1^{(t)}) = R(\alpha_2^{(t)}) = \dots = R(\alpha_l^{(t)}). \end{aligned}$$

($1 < t < n$; $lt = n$.)

Dies besagt: Ist $f(x)=0$ imprimitiv, so besitzt $f(x)$ in der Gleichung $\varphi(x)=0$ eine Tschirnhausenresolvente niedrigeren Grades.¹⁾

¹⁾ Es handelt sich hier im folgenden um eine Anwendung des Reziprozitätssatzes aus meinem Aufsatz über die Reduktion algebraischer Gleichungen

Es gilt aber auch umgekehrt: Besitzt eine irreduzible Gleichung $f(x)=0$ vom Grade n eine Tschirnhausen-resolvente niedrigeren als n -ten Grades, das heißt existiert eine rationale Funktion $R(x)$ mit Koeffizienten aus P , ist ferner a_1 irgendeine Wurzel von $f(x)=0$ und genügt $R(a_1)$ einer irreduziblen Gleichung $\varphi(x)=0$ vom Grade $l < n$, so ist $f(x)=0$ eine imprimitive Gleichung.

Seien $a_1, a_2, \dots, a_n$ die n Wurzeln von $f(x)=0$, so ist das Produkt $(x-R(a_1))(x-R(a_2)) \dots (x-R(a_n))$ als symmetrische Funktion aller Gleichungswurzeln von $f(x)=0$ im Körper P befindlich. Weiter hat dieses Produkt mit der irreduziblen Funktion $\varphi(x)$ die Nullstelle $R(a_1)$ gemeinsam. Mithin ist das fragliche Produkt durch $\varphi(x)$ teilbar.

Da aber für die Gleichung $\varphi(x)=0$ aus $\varphi(R(a_1))=0$ wegen der Irreduzibilität von $f(x)=0$ auch $\varphi(R(a_i))=0$ ($i=2, 3, \dots, n$) folgt, also $\varphi(x)$ durch sämtliche Größen $R(a_1), R(a_2), \dots, R(a_n)$ befriedigt wird, ergibt sich, wie unmittelbar ersichtlich, daß

$$(3) \quad (x-R(a_1))(x-R(a_2)) \dots (x-R(a_n)) = c \varphi(x)^l$$

werden muß, wobei c eine Konstante ist; da $\varphi(x)$ voraussetzungsgemäß von niedrigerem als n -ten Grade ist, muß $l > 1$ sein. Versteht man unter $a_1^{(1)}, a_1^{(2)}, \dots, a_1^{(t)}$ solche t Wurzeln von $f(x)=0$, die alle t untereinander verschiedenen Wurzeln $R(a_1^{(1)}), R(a_1^{(2)}), \dots, R(a_1^{(t)})$ von $\varphi(x)=0$ erschöpfen, so zerfallen infolge der Relation (3) die Wurzeln von $f(x)=0$ in t Systeme von je l untereinander gleichen:

$$\begin{aligned} & a_1^{(1)}, a_2^{(1)}, \dots, a_l^{(1)}, \\ & a_1^{(2)}, a_2^{(2)}, \dots, a_l^{(2)}, \\ & \vdots \\ & a_1^{(t)}, a_2^{(t)}, \dots, a_l^{(t)}, \end{aligned}$$

so daß $R(a_1^{(i)}) = R(a_2^{(i)}) = \dots = R(a_l^{(i)})$ ($i=1, 2, \dots, t$). Betrachtet man die zwei Gleichungen $f(x)=0$ und $R(x)-R(a_1^{(i)})=0$, so haben diese wegen der letzten l Relationen die Wurzeln $a_1^{(i)}, a_2^{(i)}, \dots, a_l^{(i)}$ und wegen der Verschiedenheit der t Wurzeln der irreduziblen Gleichung $\varphi(x)=0$, also $R(a_1^{(1)}) \neq R(a_1^{(2)}) \neq \dots \neq R(a_1^{(t)})$ auch nur die l Wurzeln $a_1^{(i)}, a_2^{(i)}, \dots, a_l^{(i)}$ gemeinsam. Der größte gemeinsame Teiler von $f(x)$ und

durch Adjunktion insbesondere reeller Radikale, Math. Zeitschrift 15 (1922), S. 262.

In der Bezeichnung des Textes ist $f(x) = c f_1(x; \vartheta_1) f_1(x; \vartheta_2) \dots f_1(x; \vartheta_t)$, $\varphi(x) = (x-\vartheta_1)(x-\vartheta_2) \dots (x-\vartheta_l)$, und der größte gemeinsame Teiler von $\varphi(x)$ und $f_1(a_h^{(i)}; x)$ ($i=1, 2, \dots, t; h=1, 2, \dots, l$) wird $x-\vartheta_i$, also $\vartheta_i = R(a_h^{(i)})$. Mithin ist $\varphi(x)^l = (x-R(a_1^{(1)}))(x-R(a_2^{(1)})) \dots (x-R(a_l^{(1)})) \dots (x-R(a_1^{(t)})) \dots (x-R(a_l^{(t)}))$, und es ist $f_1(x; \vartheta_i)$ der größte gemeinsame Teiler von $f(x)$ und $\vartheta_i - R(x)$; des weiteren $R(a_1^{(i)}) = R(a_2^{(i)}) = \dots = R(a_l^{(i)})$.

$R(x) - R(\alpha_1^{(i)})$ ist demnach $(x - \alpha_1^{(i)}) (x - \alpha_2^{(i)}) \dots (x - \alpha_t^{(i)})$. Der größte gemeinsame Teiler von $f(x)$ und $R(x) - R(\alpha_1^{(i)})$ läßt sich aber mittels des Euclidischen Algorithmus auch rational bestimmen; er hat daher Koeffizienten aus dem Körper der Koeffizienten von $f(x)$ und $R(x) - R(\alpha_1^{(i)})$, also aus dem Körper $(P; R(\alpha_1^{(i)}))$. Wir bezeichnen daher den größten gemeinsamen Teiler von $f(x)$ und $R(x) - R(\alpha_1^{(i)})$ mit $f_1(x; R(\alpha_1^{(i)}))$ und erhalten $f_1(x; R(\alpha_1^{(i)})) = (x - \alpha_1^{(i)}) (x - \alpha_2^{(i)}) \dots (x - \alpha_t^{(i)})$. Durch Multiplikation dieser für $i = 1, 2, \dots, t$ bestehenden Gleichungen folgt, da $\alpha_1^{(i)}, \alpha_2^{(i)}, \dots, \alpha_t^{(i)}$ ($i = 1, 2, \dots, t$) sämtliche $n = lt$ Wurzeln von $f(x) = 0$ erschöpfen, daß $f(x) = c f_1(x; R(\alpha_1^{(1)})) \cdot f_1(x; R(\alpha_1^{(2)})) \dots f_1(x; R(\alpha_1^{(t)}))$ wird, wobei $R(\alpha_1^{(1)}), R(\alpha_1^{(2)}), \dots, R(\alpha_1^{(t)})$ sämtliche Wurzeln von $\varphi(x) = 0$ und c eine Konstante bedeuten. Hiermit ist gezeigt, daß $f(x)$ imprimitiv im Sinne unserer Definition ist.

Mithin hat man: Charakteristisch dafür, daß $f(x) = 0$ eine imprimitive Gleichung ist, erweist sich, daß $f(x) = 0$ mindestens eine Tschirnhausenresolvente niedrigeren Grades besitzt.¹⁾

Nach dieser Charakterisierung der imprimitiven Gleichungen wenden wir uns zu dem

Satz 1. Es seien $\alpha_1, \alpha_2, \dots, \alpha_t$ irgendwelche algebraische Größen, die Gleichungen mit Koeffizienten aus P genügen. Ist das Transmutationssystem der Dirigenten $\alpha_1, \alpha_2, \dots, \alpha_t$ des Körpers $(P; \alpha_1, \alpha_2, \dots, \alpha_t)$ ein imprimitives P-Transmutationssystem der zu Beginn dieses Paragraphen beschriebenen Art, so sind $\alpha_1, \alpha_2, \dots, \alpha_t$ die Wurzeln einer und derselben imprimitiven Gleichung $f(x) = 0$ mit Koeffizienten aus P , deren weitere Wurzeln die Größen $\alpha_1^{(i)}, \alpha_2^{(i)}, \dots, \alpha_t^{(i)}$ ($i = 2, 3, \dots, t$) sind, in die sich $\alpha_1, \alpha_2, \dots, \alpha_t$ transmutieren ($t > 1$).

Zunächst enthält das Transmutationssystem der Dirigenten $\alpha_1, \alpha_2, \dots, \alpha_t$ wegen seines imprimitiven Charakters die Permutationsgruppe $\mathfrak{G}$. Da $\mathfrak{G}$ automorphe Untergruppe des Transmutationssystems ist, kann man nach Satz 3 des § 4 (I, S. 40) eine zu $\mathfrak{G}$ zugehörige rationale Funktion $\vartheta_1(\alpha_1, \alpha_2, \dots, \alpha_t)$ der Größen $\alpha_1, \alpha_2, \dots, \alpha_t$ mit Koeffizienten aus P bilden; sie nehme bei den Transmutationen $\mathfrak{G}H_i$ ($i = 2, 3, \dots, t$) die von ϑ_1 verschiedenen Werte $\vartheta_2, \vartheta_3, \dots, \vartheta_t$ an. ϑ_1 genügt dann nach Satz 1 des § 3 (I, S. 18) einer im Körper P

¹⁾ Man kann dies auch so ausdrücken: Für eine imprimitive Gleichung $f(x) = 0$ ist die Existenz zweier ganzer Funktionen $\varphi(x)$ und $R(x)$ mit Koeffizienten aus P charakteristisch, die beide von höherem als erstem Grade sind und $f(x) = \varphi(R(x))$ ergeben.

irreduziblen Gleichung $\varphi(x) = 0$, die $\vartheta_2, \vartheta_3, \dots, \vartheta_l$ zu ihren weiteren Wurzeln hat. Durch Adjunktion von ϑ_1 zum Körper P reduziert sich das Transmutationssystem der Dirigenten $a_1, a_2, \dots, a_l$ nach dem erweiterten LAGRANGESchen Satz (I, S. 22) auf diejenigen Transmutationen, die ϑ_1 ungeändert lassen, d. h. auf $\mathfrak{G}$. Bildet man nunmehr $(x-a_1)(x-a_2)\dots(x-a_l)$, so ändert sich dieser Ausdruck als symmetrische Funktion von $a_1, a_2, \dots, a_l$ bei allen Transmutationen von $\mathfrak{G}$ nicht; mithin gehört er dem Körper $(P; \vartheta_1)$ an. Man kann also setzen: $(x-a_1)(x-a_2)\dots(x-a_l) = f_1(x; \vartheta_1)$.

Wendet man auf diese richtige Gleichung zwischen $a_1, a_2, \dots, a_l$ mit Koeffizienten aus P — auch ϑ_1 ist ja rationale Funktion von $a_1, a_2, \dots, a_l$ — die Transmutationen H_i ($i = 2, 3, \dots, l$) der Dirigenten $a_1, a_2, \dots, a_l$ an, so erhält man die weiteren richtigen Gleichungen:

$$(x-a_1^{(i)})(x-a_2^{(i)})\dots(x-a_l^{(i)}) = f_1(x; \vartheta_i) \quad (i = 2, 3, \dots, l)$$

und durch ihre Multiplikation:

$$\begin{aligned} (x-a_1)(x-a_2)\dots(x-a_l)\dots(x-a_1^{(i)})(x-a_2^{(i)})\dots(x-a_l^{(i)}) \\ = f_1(x; \vartheta_1)f_1(x; \vartheta_2)\dots f_1(x; \vartheta_l). \end{aligned}$$

Die rechte Seite ist eine symmetrische Funktion von $\vartheta_1, \vartheta_2, \dots, \vartheta_l$, mithin durch die Koeffizienten von $\varphi(x) = 0$ darstellbar und kann daher mit $f(x)$ bezeichnet werden, wobei $f(x)$ nur Koeffizienten aus P enthält.

Nachdem die Zerlegbarkeit von $f(x)$ dargetan ist, hat man zum Nachweis der Imprimitivität von $f(x)$ nur noch zu zeigen, daß $f(x)$ in P irreduzibel ist. Sei etwa $F(x)$ der irreduzible Faktor von $f(x)$, der durch a_1 befriedigt wird, also $F(a_1) = 0$. Da $\mathfrak{G}$ infolge seines transitiven Charakters l Permutationen $P_1, P_2, \dots, P_l$ enthält, die a_1 sukzessiv in $a_1, a_2, \dots, a_l$ überführen, folgt aus der Gleichung $F(a_1) = 0$ durch Anwendung dieser Permutationen weiter $F(a_2) = 0, F(a_3) = 0, \dots, F(a_l) = 0$. Da das Transmutationssystem der Dirigenten $a_1, a_2, \dots, a_l$ voraussetzungsgemäß auch die Transmutationen

$$H_i = \begin{pmatrix} a_1 & a_2 & \dots & a_l \\ a_1^{(i)} & a_2^{(i)} & \dots & a_l^{(i)} \end{pmatrix}$$

besitzt, so geht $F(a_1) = 0$ durch die Transmutationen $P_1 H_i, P_2 H_i, \dots, P_l H_i$ in $F(a_1^{(i)}) = 0, F(a_2^{(i)}) = 0, \dots, F(a_l^{(i)}) = 0$ über. Es wird also $F(x) = 0$ durch alle Wurzeln von $f(x) = 0$ befriedigt, d. h. $f(x) = 0$ ist selbst in P irreduzibel.

Als Umkehrung von Satz 1 beweisen wir den

Satz 2. Ist $f(x) = 0$ eine imprimitive Gleichung mit Koeffizienten aus P vom Grade n , so kann man unter

ihren Wurzeln stets l ($1 < l < n$): $a_1, a_2, \dots, a_l$ so auswählen, daß diese Dirigenten für ein imprimitives Transmutationssystem sind.

Nach Voraussetzung ist $f(x) = 0$ imprimitiv, also $f(x)$ zerlegbar in

$$(2) \quad f(x) = c f_1(x; \vartheta_1) f_1(x; \vartheta_2) \dots f_1(x; \vartheta_t),$$

wobei $\vartheta_i = R(a_1^{(i)}) = R(a_2^{(i)}) = \dots = R(a_l^{(i)})$ ($i = 1, 2, \dots, t$), $a_1^{(i)}, a_2^{(i)}, \dots, a_l^{(i)}$ ($i = 1, 2, \dots, t$) alle Wurzeln von $f(x) = 0$ und $\vartheta_1, \vartheta_2, \dots, \vartheta_t$ alle Wurzeln der in P irreduziblen Gleichung $\varphi(x) = 0$ vom Grade $t = \frac{n}{l}$ bedeuten. Wir behaupten: Jedes System von Wurzeln einer der t Gleichungen $f_1(x; \vartheta_i) = 0$ liefert, wenn man es zum Dirigentensystem wählt, ein imprimitives Transmutationssystem. Wir nehmen die Wurzeln $a_1, a_2, \dots, a_l$ von $f_1(x; \vartheta_1) = 0$ als Dirigenten des Körpers $(P; a_1, a_2, \dots, a_l)$. Da jede richtige Gleichung mit Koeffizienten aus P durch die Transmutationen eines Transmutationssystems wieder in eine richtige Gleichung übergeht, folgt aus $f(a_h) = 0$ ($h = 1, 2, \dots, l$), daß jede der Wurzeln $a_1, a_2, \dots, a_l$ bei allen Transmutationen wieder in eine Wurzel von $f(x) = 0$ übergeführt wird. Weiter ergibt sich aus $\varphi(R(a_h)) = 0$ ($h = 1, 2, \dots, l$), daß durch die Transmutationen von $a_1, a_2, \dots, a_l$ sich stets $R(a_1) = R(a_2) = \dots = R(a_l)$ nur in Wurzeln von $\varphi(x) = 0$ transmutieren kann, also in eine der Größen der folgenden t Reihen:

$$R(a_1^{(i)}) = R(a_2^{(i)}) = \dots = R(a_l^{(i)}) \quad (i = 1, 2, \dots, t).$$

Wir betrachten von dem Transmutationssystem der Dirigenten $a_1, a_2, \dots, a_l$ zunächst diejenigen, bei denen sich $R(a_1)$ nicht ändert. Sie führen alle richtigen Gleichungen zwischen $a_1, a_2, \dots, a_l$ mit Koeffizienten aus $(P; R(a_1))$ wieder in solche über und bilden daher die GALOISSche Gruppe $\mathfrak{G}$ der Gleichung $f_1(x; R(a_1)) = 0$ mit den Wurzeln $a_1, a_2, \dots, a_l$. Als GALOISSche Gruppe einer Gleichung ist $\mathfrak{G}$ Permutationsgruppe und weiter ist $\mathfrak{G}$ wegen der Irreduzibilität von $f_1(x; R(a_1))$ im Körper $(P; R(a_1))$ transitiv.¹⁾

Mit der Permutationsgruppe $\mathfrak{G}$ der Größen $a_1, a_2, \dots, a_l$ kann nicht ihr ganzes Transmutationssystem erschöpft sein; denn wegen

¹⁾ Wäre $f_1(x; \vartheta_1)$ reduzibel und besäße den Faktor $F_1(x; \vartheta_1)$, so wäre $f(x)$ durch das Produkt $F_1(x; \vartheta_1) F_1(x; \vartheta_2) \dots F_1(x; \vartheta_t)$ teilbar und daher im Widerspruch zur Imprimitivität von $f(x)$ im Körper P reduzibel. Da $f_1(x; \vartheta_1)$ irreduzibel ist, hat man nach der im § 1 gegebenen Vorschrift zur Bildung eines beliebigen Transmutationssystems a_1 durch alle Wurzeln von $f_1(x; \vartheta_1)$, das heißt sukzessiv durch $a_1, a_2, \dots, a_l$ zu ersetzen; und dies bedeutet die Transitivität von $\mathfrak{G}$.

$R(a_1) = R(a_2) = \dots = R(a_l)$ läßt $f_1(x; R(a_1))$ alle Permutationen von $\mathfrak{G}$ zu. Würde $\mathfrak{G}$ das Transmutationssystem der Dirigenten $a_1, a_2, \dots, a_l$ für den Körper P erschöpfen, so würde $f_1(x; R(a_1))$ Koeffizienten aus P haben und müßte im Widerspruch zu $t > 1$ mit der wegen der Imprimitivität irreduziblen Funktion $f(x)$ zusammenfallen. Π_i sei eine Transmutation der Dirigenten $a_1, a_2, \dots, a_l$, die $\mathfrak{G}$ nicht angehöre und $a_1, a_2, \dots, a_l$ in $\bar{a}_1, \bar{a}_2, \dots, \bar{a}_l$ überführe. Die Anwendung dieser Transmutation auf die richtigen Gleichungen $R(a_1) = R(a_2) = \dots = R(a_l)$ liefert $R(\bar{a}_1) = R(\bar{a}_2) = \dots = R(\bar{a}_l)$. Da die Transmutationen der Dirigenten $a_1, a_2, \dots, a_l$ diese Größen nur in Wurzeln von $f(x) = 0$ und weiter dabei $R(a_1), R(a_2), \dots, R(a_l)$ in Wurzeln von $\varphi(x) = 0$ überführen, wie oben auseinandergesetzt wurde, müssen $\bar{a}_1, \bar{a}_2, \dots, \bar{a}_l$ solche l Wurzeln von $f(x)$ sein, für die $R(x)$ gleiche Werte

$$R(a_1^{(i)}) = R(a_2^{(i)}) = \dots = R(a_l^{(i)}) \quad (i = 2, 3, \dots, t)$$

annimmt. Man kann also $\bar{a}_1 = a_1^{(i)}, \bar{a}_2 = a_2^{(i)}, \dots, \bar{a}_l = a_l^{(i)}$ setzen und gewinnt $\Pi_i = \begin{pmatrix} a_1 & a_2 & \dots & a_l \\ a_1^{(i)} & a_2^{(i)} & \dots & a_l^{(i)} \end{pmatrix}$. Entsprechend den t Wurzeln von $\varphi(x) = 0$ existieren auch außer der identischen Transmutation noch $t-1$ verschiedene Transmutationen Π_i ($i = 2, 3, \dots, t$); denn würde das Transmutationssystem der Dirigenten $a_1, a_2, \dots, a_l$ nur Transmutationen $\Pi_2, \Pi_3, \dots, \Pi_s$ haben, wo s kleiner als die Anzahl t der Wurzeln von $\varphi(x) = 0$ ist, so würde nach dem Satz 1 $f(x)$ einen irreduziblen Faktor niedrigeren Grades mit Koeffizienten aus P besitzen. Hiermit ist der Satz 2 bewiesen.

Aus den Sätzen 1 und 2 folgt der

Satz 3. Charakteristisch für imprimitive Gleichungen $f(x) = 0$ vom n -ten Grade ist, daß man aus ihren Wurzeln l ($1 < l < n$) herausgreifen kann, die Dirigenten eines imprimitiven P -Transmutationssystems sind.

Aus dem Satz 3 folgt unmittelbar die übliche Definition der imprimitiven Gleichungen als Theorem, nämlich der

Satz 4. Eine irreduzible Gleichung $f(x) = 0$ ist dann und nur dann imprimitiv, wenn ihre GALOISsche Gruppe imprimitiv ist.¹⁾

¹⁾ Mit imprimitiven Permutationsgruppen haben sich bereits P. RUFFINI, CAUCHY und E. GALOIS beschäftigt. Eine Behandlung imprimitiver Gleichungen, ausgehend von der Imprimitivität ihrer GALOISschen Gruppen bei C. JORDAN, *Traité des substitutions et des équations algébriques*, Paris 1870, S. 259 sowie bei H. WEBER, *Lehrbuch der Algebra*, Bd. 1, S. 524, 2. Aufl., Braunschweig 1898; WEBER hat auch a. a. O. S. 504 den Begriff des primitiven und imprimitiven Körpers eingeführt.

Der Beweis ergibt sich sofort aus der folgenden allgemeinen Bemerkung: Ist $\varrho_1, \varrho_2, \dots, \varrho_h$ ein Teilsystem der Größen $\varrho_1, \varrho_2, \dots, \varrho_k$, die, wie im § 1 (I, S. 4) durch die Gleichungskette

$$X_1(x) = 0, X_2(x; \varrho_1) = 0, \dots, X_k(x; \varrho_1, \varrho_2, \dots, \varrho_{k-1}) = 0$$

gegeben seien, so findet man das Transmutationsystem der Dirigenten $\varrho_1, \varrho_2, \dots, \varrho_h$ des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_h)$ nach der in § 1 gegebenen Vorschrift aus den ersten h Gleichungen, indem man sich auf diese beschränkt. Aus jeder Transmutation $\begin{pmatrix} \varrho_1 & \varrho_2 & \dots & \varrho_k \\ \varrho_{1i} & \varrho_{2i} & \dots & \varrho_{ki} \end{pmatrix}$ der Dirigenten $\varrho_1, \varrho_2, \dots, \varrho_k$ des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ ergibt sich demnach eine Transmutation der Größen $\varrho_1, \varrho_2, \dots, \varrho_h$, indem man im Zähler $\varrho_{h+1}, \varrho_{h+2}, \dots, \varrho_k$ und die unter ihnen stehenden Größen des Nenners streicht. Auf diese Weise erhält man auch sämtliche Transmutationen der Dirigenten $\varrho_1, \varrho_2, \dots, \varrho_h$ des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_h)$.

Ist die GALOISSche Gruppe von $f(x) = 0$ imprimitiv, so heißt dies: Man kann die n Wurzeln von $f(x) = 0$ in t ($t > 1$) Systeme zu je l einteilen: $\alpha_1, \alpha_2, \dots, \alpha_l, \alpha_1^{(i)}, \alpha_2^{(i)}, \dots, \alpha_l^{(i)}$ ($i = 2, 3, \dots, t$), die sich als Ganzes untereinander permutieren, und es geht hierbei jede Wurzel in jede über. Diese Tatsache bedeutet aber, wenn man sich auf $\alpha_1, \alpha_2, \dots, \alpha_l$ beschränkt, daß diese Größen ein imprimitives P-Transmutationssystem erleiden. Ist umgekehrt eine Gleichung n -ten Grades $f(x) = 0$ imprimitiv, so lassen sich ihre Wurzeln in t Systeme zu je l teilen: $\alpha_1, \alpha_2, \dots, \alpha_l, \alpha_1^{(i)}, \alpha_2^{(i)}, \dots, \alpha_l^{(i)}$ ($i = 2, 3, \dots, t$), so daß $\alpha_1, \alpha_2, \dots, \alpha_l$ Dirigenten eines imprimitiven P-Transmutationssystems werden. Das nämliche trifft auch für jedes der mit $\alpha_1, \alpha_2, \dots, \alpha_l$ gleichberechtigten $t-1$ Systeme $\alpha_1^{(i)}, \alpha_2^{(i)}, \dots, \alpha_l^{(i)}$ ($i = 2, 3, \dots, t$) zu. Diese Tatsachen bedeuten aber nach der oben gemachten Vorbemerkung, daß sich bei den Transmutationen aller Wurzeln der Gleichung $f(x) = 0$, das heißt bei ihrer GALOISSchen Gruppe, die t Systeme stets gesondert in sich oder als Ganzes ineinander permutieren, also die GALOISSche Gruppe von $f(x) = 0$ imprimitiv ist.

Definition der primitiven Gleichung: Jede irreduzible Gleichung mit Koeffizienten aus P , die nicht imprimitiv ist, heißt primitiv.

Definition des primitiven und imprimitiven Körpers: Der Körper $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$, bei dem $\varrho_1, \varrho_2, \dots, \varrho_k$ durch eine Gleichungskette wie im § 1 (I, S. 4) definiert seien, heißt primitiv oder imprimitiv, je nachdem jede rationale Funktion von $\varrho_1, \varrho_2, \dots, \varrho_k$ mit Koeffizienten aus P einer in P irreduziblen Gleichung s -ten Grades genügt oder es auch

rationale Funktionen von $\varrho_1, \varrho_2, \dots, \varrho_k$ mit Koeffizienten aus P gibt, die Gleichungen niedrigeren als s -ten Grades mit Koeffizienten aus P genügen; dabei ist s die Anzahl der Transmutationen der Dirigenten $\varrho_1, \varrho_2, \dots, \varrho_k$ oder der Grad des Körpers. Anders ausgedrückt: Ein primitiver Körper $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ enthält keine echten Unterkörper als in P befindliche; ein imprimitiver Körper enthält stets solche.

Im Falle des primitiven Körpers kann die Gleichungskette $X_1(x) = 0, X_2(x; \varrho_1) = 0, \dots, X_k(x; \varrho_1, \varrho_2, \dots, \varrho_{k-1}) = 0$ nur eine einzige Gleichung enthalten, die nicht vom ersten Grade ist; diese Gleichung hat den Grad s . Wäre nämlich $X_h(x; \varrho_1, \varrho_2, \dots, \varrho_{h-1}) = 0$ ($h < k$) die erste Gleichung von höherem als erstem, aber niedrigerem als s -tem Grade, so würde sich die Größe ϱ_h im Widerspruch mit der Primitivität des Körpers befinden. Der primitive Körper läßt sich auch so charakterisieren: Jede rationale Funktion seiner Dirigenten $\varrho_1, \varrho_2, \dots, \varrho_k$ gehört zur identischen Transmutation E , ändert sich also bei jeder von dieser verschiedenen Transmutation in ihrem Wert. Man kann dies auch so ausdrücken: Jede nicht P selbst angehörige Größe eines primitiven Körpers ist primitiv und genügt stets einer primitiven Gleichung mit Koeffizienten aus P [vgl. § 4 (I, S. 41)].

Würde nämlich bei einem primitiven Körper eine Gleichung, die durch eine rationale Funktion von $\varrho_1, \varrho_2, \dots, \varrho_k$ befriedigt wird, eine Tschirnhausenresolvente von niedrigerem als s -tem Grade besitzen, also eine imprimitive Gleichung sein, so gäbe es im Körper $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ im Gegensatz zu seiner Primitivität rationale Funktionen von $\varrho_1, \varrho_2, \dots, \varrho_k$, die selbst Gleichungen niedrigeren Grades als des Körpergrades s befriedigen.

Wir betrachten nunmehr einen imprimitiven Körper $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$. Es bedeute σ_e eine diesen Körper erzeugende, also primitive Größe, die demnach einer in P irreduziblen Gleichung s -ten Grades genüge. Wegen der Imprimitivität des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ besitzt der Körper rationale Funktionen von $\varrho_1, \varrho_2, \dots, \varrho_k$, das heißt, da σ_e primitive Größe des Körpers ist (vgl. § 4, I, S. 41), auch rationale Funktionen von σ_e , die Wurzeln von Gleichungen niedrigeren als s -ten Grades mit Koeffizienten aus P sind. Da die durch σ_e befriedigte Gleichung demnach Tschirnhausenresolventen niedrigeren Grades besitzt, ist die durch σ_e erfüllte Gleichung imprimitiv. Wir wollen daher die primitiven Funktionen von $\varrho_1, \varrho_2, \dots, \varrho_k$ bei einem imprimitiven

Körper schwach primitiv nennen. Wir erhalten demnach das Resultat: Jede primitive GröÙe eines imprimitiven Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ ist schwach primitiv und genügt einer imprimitiven Gleichung.

Hat man einen imprimitiven Körper $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$, so genügt jede seiner primitiven GröÙen, von denen eine mit α_1 bezeichnet sei, einer imprimitiven Gleichung $f(x) = 0$ vom Körpergrade. Nach dem Charakter der imprimitiven Gleichung existiert dann eine rationale Funktion $R(\alpha_1)$ von α_1 mit Koeffizienten aus P , so daß $\vartheta_1 = R(\alpha_1)$ die Wurzel einer irreduziblen Gleichung $\varphi(x) = 0$ mit Koeffizienten aus P und α_1 die Wurzel einer in $(P; \vartheta_1)$ irreduziblen Gleichung $f_1(x; \vartheta_1) = 0$ wird, wobei das Produkt der Grade von $\varphi(x) = 0$ und $f_1(x; \vartheta_1) = 0$ gleich dem Körpergrade ist. ϑ_1, α_1 erzeugen demnach auch den Körper $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$. Mithin ergibt sich der Satz: Für den imprimitiven Körper ist charakteristisch, daß man bei ihm stets ein Dirigentensystem $\varrho_1, \varrho_2, \dots, \varrho_k$ so auswählen kann, daß diese Dirigenten $\varrho_1, \varrho_2, \dots, \varrho_k$ des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ der Reihe nach den Gleichungen $X_1(x) = 0, X_2(x; \varrho_1) = 0, \dots, X_k(x; \varrho_1, \varrho_2, \dots, \varrho_{k-1}) = 0$ genügen, die in den Körpern P beziehungsweise $(P; \varrho_1), (P; \varrho_1, \varrho_2), \dots, (P; \varrho_1, \varrho_2, \dots, \varrho_{k-1})$ irreduzibel sind und von denen mindestens zwei Gleichungen höheren als ersten Grad besitzen. Man kann es dabei so einrichten, indem man ϱ_k als erzeugende Funktion des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ wählt, daß jede folgende Gleichung Koeffizienten aus einem wirklichen Erweiterungskörper der Koeffizienten der vorausgehenden Gleichung enthält.

Da es für den imprimitiven Körper $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ und nur für ihn stets rationale Funktionen $\sigma_1(\varrho_1, \varrho_2, \dots, \varrho_k)$ gibt, die Gleichungen niedrigeren Grades als des Körpergrades s genügen, folgt nach Satz 1 und 2 des § 3 (I, S. 18 und 21):

Charakteristisch für den imprimitiven Körper $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ ist, daß es für ihn rationale Funktionen $\sigma_1(\varrho_1, \varrho_2, \dots, \varrho_k)$ gibt, die bei einem echten, von der Identität verschiedenen Teilsystem $\mathfrak{S}_1$ des Transmutationsystems $\mathfrak{S}$ des Körpers $(P; \varrho_1, \varrho_2, \dots, \varrho_k)$ ungeändert bleiben. Die Zahl s_1 der Transmutationen von $\mathfrak{S}_1$ ist echter Teiler von s .

(Fortsetzung folgt.)