

Werk

Titel: Journal für die reine und angewandte Mathematik

Verlag: de Gruyter

Jahr: 1892

Kollektion: Mathematica

Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen

Werk Id: PPN243919689_0110

PURL: http://resolver.sub.uni-goettingen.de/purl?PPN243919689_0110

LOG Id: LOG_0009

LOG Titel: Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten.

LOG Typ: article

Übergeordnetes Werk

Werk Id: PPN243919689

PURL: <http://resolver.sub.uni-goettingen.de/purl?PPN243919689>

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.

Each copy of any part of this document must contain there Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.

Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten.

(Von Herrn *David Hilbert* in Königsberg i. Pr.)

Wenn eine ganze rationale Function mit ganzzahligen Coefficienten und mit den Veränderlichen $x, y, \dots, w; t, r, \dots, q$ vorgelegt ist und wir behalten in dieser Function einige von den Veränderlichen, etwa die Veränderlichen $x, y, \dots, w$, als Unbestimmte bei, während wir für die übrigen Veränderlichen $t, r, \dots, q$ irgend welche ganze positive oder negative Zahlen einsetzen, so entsteht ein System von unbegrenzt vielen ganzen rationalen Functionen der Veränderlichen $x, y, \dots, w$ mit ganzzahligen Coefficienten, und wir werden auf die Frage geführt, ob in diesem Systeme nothwendig irreducible Functionen der Veränderlichen $x, y, \dots, w$ vorhanden sein müssen, sobald die ursprünglich vorgelegte Function eine irreducible Function der Veränderlichen $x, y, \dots, w; t, r, \dots, q$ ist. Dabei wird eine ganze rationale Function mit ganzzahligen Coefficienten irreducibel genannt, wenn sie nicht als Product mehrerer solcher ganzer ganzzahliger Functionen darstellbar ist. Die angeregte Frage und ihre Erweiterung auf beliebige Rationalitätsbereiche rückt den Begriff der Irreducibilität in ein neues Licht, und überdies gestatten die sich ergebenden Resultate mannigfache besondere Anwendungen auf die Theorie der Gleichungen und der Rationalitätsbereiche.

Unsere Entwicklungen beruhen auf folgendem Hilfssatze:

Es sei eine unendliche Zahlenreihe $a_1, a_2, a_3, \dots$ vorgelegt, in welcher allgemein a , eine der a ganzen positiven Zahlen $1, 2, \dots, a$ bedeutet; es sei überdies m irgend eine ganze positive Zahl. Dann lassen sich stets m ganze positive Zahlen $\mu^{(1)}, \mu^{(2)}, \dots, \mu^{(m)}$ so bestimmen, dass die 2^m Elemente

$$\begin{array}{ccccccc}
a_{\mu}, & & & & & & \\
a_{\mu+\mu^{(1)}}, & & & & & & \\
a_{\mu+\mu^{(2)}}, & a_{\mu+\mu^{(1)}+\mu^{(2)}}, & & & & & \\
a_{\mu+\mu^{(3)}}, & a_{\mu+\mu^{(1)}+\mu^{(3)}}, & a_{\mu+\mu^{(2)}+\mu^{(3)}}, & a_{\mu+\mu^{(1)}+\mu^{(2)}+\mu^{(3)}}, & & & \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
a_{\mu+\mu^{(m)}}, & a_{\mu+\mu^{(1)}+\mu^{(m)}}, & a_{\mu+\mu^{(2)}+\mu^{(m)}}, & \cdot & \cdot & \cdot, & a_{\mu+\mu^{(1)}+\mu^{(2)}+\dots+\mu^{(m)}}
\end{array}$$

für unendlich viele ganzzahlige Werthe μ sämmtlich gleich der nämlichen Zahl G sind, wo G eine der Zahlen $1, 2, \dots, a$ bedeutet. Dabei wird der Index $\mu + \mu^{(1)}$ des zweiten Elementes erhalten, indem man die Zahl $\mu^{(1)}$ zu dem Index μ des ersten Elementes addirt; die Indices des dritten und vierten Elementes entstehen aus den Indices des ersten und zweiten Elementes, indem man zu diesen die Zahl $\mu^{(2)}$ addirt; die Indices des fünften, sechsten, siebenten, achten Elementes entstehen aus den Indices der vier ersten Elemente, wenn man zu diesen die Zahl $\mu^{(3)}$ addirt, und schliesslich erhält man die Indices der 2^{m-1} letzten Elemente, indem man zu den schon bestimmten Indices der 2^{m-1} ersten Elemente die Zahl $\mu^{(m)}$ addirt.

Beim Beweise ist es nothwendig, einzelne Theile der vorgelegten Reihe für sich zu betrachten. Wenn insbesondere i auf einander folgende Elemente der Reihe herausgegriffen werden, etwa die Elemente $a_\mu, a_{\mu+1}, a_{\mu+2}, \dots, a_{\mu+i-1}$, so nenne ich diese i Elemente ein Intervall der Reihe von der Länge i . Wir grenzen nun innerhalb der vorgelegten Reihe irgend ein Intervall von der Länge $a+1$ ab. In diesem Intervalle tritt dann mindestens eine der Zahlen $1, 2, \dots, a$, etwa die Zahl G , zweimal auf, d. h. in dem Intervalle von der Länge $a+1$ kommt jedenfalls eine der folgenden Gruppierungen vor:

$$\begin{aligned} G_2^{(1)} &= GG, \\ G_3^{(1)} &= G.G, \\ G_4^{(1)} &= G..G, \\ &\vdots \\ G_{a+1}^{(1)} &= G... \dots ..G. \end{aligned}$$

Wie schon durch die Schreibweise kenntlich gemacht ist, bedeutet hierin allgemein $G_s^{(1)}$ ein Intervall von der Länge s , dessen erstes und letztes Element einander gleich, nämlich gleich der Zahl G sind. Man sieht, dass die Anzahl aller möglichen von einander verschiedenen Gruppierungen $G_s^{(1)}$

wird. Aus dem Aufbau der Gruppierung $G_{\nu(m)}^{(m)}$ folgt dann

$$a_{\mu} = G,$$

$$a_{\mu+\mu(1)} = G,$$

$$a_{\mu+\mu(2)} = a_{\mu+\mu(1)+\mu(2)} = G,$$

$$a_{\mu+\mu(3)} = a_{\mu+\mu(1)+\mu(3)} = a_{\mu+\mu(2)+\mu(3)} = a_{\mu+\mu(1)+\mu(2)+\mu(3)} = G,$$

$$\dots \dots \dots$$

$$a_{\mu+\mu(m)} = a_{\mu+\mu(1)+\mu(m)} = a_{\mu+\mu(2)+\mu(m)} = \dots = a_{\mu+\mu(1)+\mu(2)+\dots+\mu(m)} = G,$$

und damit ist der Hilfssatz bewiesen.

Wir kehren jetzt zu der anfangs gestellten Frage zurück und beweisen zunächst das folgende Theorem:

I. Wenn $f(x, t)$ eine irreducible ganze rationale Function der beiden Veränderlichen x und t mit ganzzahligen Coefficienten bezeichnet, so ist es stets auf unendlich viele Weisen möglich, in $f(x, t)$ für t eine ganze rationale Zahl einzusetzen, so dass dadurch die Function $f(x, t)$ in eine irreducible Function der einen Veränderlichen x übergeht. Dabei heisst eine ganze rationale Function mit ganzzahligen Coefficienten irreducible, wenn sie nicht als Product mehrerer solcher Functionen mit ganzzahligen Coefficienten dargestellt werden kann.

Wir setzen

$$f(x, t) = Tx^n + T_1x^{n-1} + \dots + T_n,$$

wo $T, T_1, \dots, T_n$ ganze rationale Functionen von t mit ganzzahligen Coefficienten sind, und nehmen dann — im Gegensatze zu der in obigem Theoreme ausgesprochenen Behauptung — an, dass die Function $f(x, t)$ stets gleich einem Producte zweier oder mehrerer ganzer ganzzahliger Functionen von x wird, sobald wir für t irgend eine ganze positive, oberhalb einer bestimmten Grenze C gelegene Zahl einsetzen. Vermöge der Substitution $x = \frac{y}{T}$ erhalten wir

$$f(x, t) = \frac{1}{T^{n-1}} \{y^n + S_1y^{n-1} + S_2y^{n-2} + \dots + S_n\},$$

wo $S_1, S_2, \dots, S_n$ wiederum ganze ganzzahlige Functionen von t bedeuten, und es wird dann auch die Function

$$g(y, t) = y^n + S_1y^{n-1} + S_2y^{n-2} + \dots + S_n$$

reducibel für jeden positiven ganzzahligen Werth von t , welcher eine gewisse Grenze C' überschreitet, wo $C' \geq C$ und überdies so gross gewählt

von je zwei Potenzreihen. Wir wählen ferner aus den n Wurzeln $y_1, y_2, \dots, y_n$ irgend drei aus, etwa y_1, y_2, y_3 , und bilden dann die Potenzreihen für die drei elementarsymmetrischen Functionen derselben, wie folgt

$$\begin{aligned} y_1 + y_2 + y_3 &= (\alpha_1 + \alpha_2 + \alpha_3)\tau^h + (\beta_1 + \beta_2 + \beta_3)\tau^{h-1} + \dots, \\ y_1 y_2 + y_1 y_3 + y_2 y_3 &= (\alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_2 \alpha_3)\tau^{2h} \\ &\quad + (\alpha_1 \beta_2 + \alpha_2 \beta_1 + \alpha_1 \beta_3 + \alpha_3 \beta_1 + \alpha_2 \beta_3 + \alpha_3 \beta_2)\tau^{2h-1} + \dots, \\ y_1 y_2 y_3 &= \alpha_1 \alpha_2 \alpha_3 \tau^{3h} + (\alpha_1 \alpha_2 \beta_3 + \alpha_1 \alpha_3 \beta_2 + \alpha_2 \alpha_3 \beta_1)\tau^{3h-1} + \dots. \end{aligned}$$

Da wir auf $\binom{n}{3}$ Weisen je drei Wurzeln aus den n Wurzeln $y_1, y_2, \dots, y_n$ auswählen können, so ergeben sich im Ganzen $\binom{n}{3}$ Systeme von je drei Potenzreihen. In derselben Weise gelangen wir zu $\binom{n}{4}$ Systemen von je vier Potenzreihen, zu $\binom{n}{5}$ Systemen von je fünf Potenzreihen u. s. f. Schliesslich wählen wir unter den n Wurzeln $y_1, y_2, \dots, y_n$ irgend $n-1$ aus etwa $y_1, y_2, \dots, y_{n-1}$ und bilden die Potenzreihen für die $n-1$ elementarsymmetrischen Functionen derselben, wie folgt

$$\begin{aligned} y_1 + y_2 + \dots + y_{n-1} &= (\alpha_1 + \alpha_2 + \dots + \alpha_{n-1})\tau^h + (\beta_1 + \beta_2 + \dots + \beta_{n-1})\tau^{h-1} + \dots, \\ y_1 y_2 \dots y_{n-1} &= \alpha_1 \alpha_2 \dots \alpha_{n-1} \tau^{(n-1)h} \\ &\quad + (\alpha_1 \alpha_2 \dots \alpha_{n-2} \beta_{n-1} + \dots + \alpha_2 \alpha_3 \dots \alpha_{n-1} \beta_1)\tau^{(n-1)h-1} + \dots. \end{aligned}$$

Es ergeben sich auf diese Weise $\binom{n}{n-1} = n$ Systeme, von denen jedes aus $n-1$ Potenzreihen besteht.

Wenn wir jetzt noch die n ursprünglichen Potenzreihen hinzunehmen und jede von diesen für sich als ein System zählen, so haben wir insgesamt $n + \binom{n}{2} + \binom{n}{3} + \dots + \binom{n}{n-1} = 2^n - 2$ Systeme von Potenzreihen. Diese $2^n - 2$ Systeme von Potenzreihen wollen wir in eine bestimmte Reihenfolge bringen und mit den Nummern 1, 2, $\dots$, $2^n - 2$ versehen.

Nachdem dies geschehen ist, bestimmen wir eine Primzahl p , welche grösser ist als jede der beiden Grössen C' und C'' , und denken uns dann in sämtliche Potenzreihen unserer $2^n - 2$ Systeme für τ den positiven reellen Werth von $p^{\frac{1}{k}}$ eingesetzt. Da unserer früheren Annahme zufolge die ganze ganzzahlige Function $g(y, p)$ reducibel wird, d. h. in zwei ganze

sämmtlich gleich Null, und es bezeichne $\frac{V_1}{\sigma^v}$ das erste Glied, dessen Coefficient V_1 nicht verschwindet. Wir erhalten dann

$$\mathfrak{P}^{(1)}(\sigma) = \varphi_{m-1}(\sigma) - \varphi_{m-1}(\sigma + \mu^{(1)}) + V_1 \left[\frac{1}{\sigma^v} - \frac{1}{(\sigma + \mu^{(1)})^v} \right] + \dots$$

Hier ist die erste auf der rechten Seite stehende Differenz eine ganze rationale Function vom $(m-2)$ ten Grade in σ ; wir setzen

$$\varphi_{m-2}(\sigma) = \varphi_{m-1}(\sigma) - \varphi_{m-1}(\sigma + \mu^{(1)}).$$

Die übrigen Glieder auf der rechten Seite entwickeln wir nach fallenden Potenzen von σ ; es wird dann

$$\mathfrak{P}^{(1)}(\sigma) = \varphi_{m-2}(\sigma) + \mu^{(1)} v \frac{V_1}{\sigma^{v+1}} + \dots$$

In entsprechender Weise erhalten wir

$$\mathfrak{P}^{(2)}(\sigma) = \varphi_{m-3}(\sigma) + \mu^{(1)} \mu^{(2)} v(v+1) \frac{V_1}{\sigma^{v+2}} + \dots,$$

wo $\varphi_{m-3}(\sigma)$ eine ganze rationale Function vom $(m-3)$ ten Grade in σ bedeutet. Nach m Schritten gelangen wir schliesslich zu der Formel

$$\mathfrak{P}^{(m)}(\sigma) = \mu^{(1)} \mu^{(2)} \dots \mu^{(m)} v(v+1) \dots (v+m-1) \frac{V_1}{\sigma^{v+m}} + \dots$$

Da diese Potenzreihe mit negativen Potenzen von σ beginnt, so lässt sich eine positive Grösse F angeben derart, dass für alle diese Grenze F überschreitenden Werthe von σ der Werth der Potenzreihe absolut genommen kleiner als Eins ausfällt. Andererseits wird die Potenzreihe $\mathfrak{P}^{(m)}(\sigma)$ für unendlich viele ganzzahlige Argumente σ selbst gleich einer ganzen Zahl, und da eine ganze Zahl, deren absoluter Betrag unterhalb der Einheit liegt, nothwendig gleich Null sein muss, so folgt, dass es unendlich viele ganzzahlige Werthe von σ giebt, für welche die Potenzreihe $\mathfrak{P}^{(m)}(\sigma)$ verschwindet.

Aus der letzten Formel ergibt sich aber

$$\lim_{\sigma \rightarrow \infty} [\sigma^{v+m} \mathfrak{P}^{(m)}(\sigma)] = \mu^{(1)} \mu^{(2)} \dots \mu^{(m)} v(v+1) \dots (v+m-1) V_1,$$

wo der Ausdruck rechter Hand eine von Null verschiedene Grösse darstellt. Dieser Umstand steht mit der eben bewiesenen Thatsache in Widerspruch, und es ist daher unmöglich, dass unter den Coefficienten $P_1, R_1, S_1, \dots$ ein von Null verschiedener Coefficient V_1 auftritt. In derselben Weise folgt, dass auch die Coefficienten $P_2, R_2, S_2, \dots, P_v, R_v, S_v, \dots$ sämmtlich

T eine ganze ganzzahlige Function der einen Veränderlichen t ist. Bezeichnet dann P irgend eine in A oder in sämtlichen Coefficienten von T aufgehende Primzahl, so wird der Quotient

$$\frac{\Phi(x, t)\Phi'(x, t)}{P}$$

gleich einer ganzen ganzzahligen Function von x und t , und hieraus folgt leicht durch bekannte Schlüsse, dass entweder die sämtlichen Coefficienten von $\Phi(x, t)$ oder diejenigen von $\Phi'(x, t)$ durch P theilbar sein müssen. Wenn ferner $U(t)$ eine ganze ganzzahlige irreducible in T aufgehende Function von t bezeichnet, so wird der Quotient

$$\frac{\Phi(x, t)\Phi'(x, t)}{U(t)}$$

ebenfalls gleich einer ganzen ganzzahligen Function von x und t , und hieraus folgt in ähnlicher Weise, dass entweder in $\Phi(x, t)$ oder in $\Phi'(x, t)$ die sämtlichen Potenzen von x mit Functionen von t multiplicirt sind, welche die Function $U(t)$ als Factor enthalten. Durch Fortheben der sämtlichen Primzahlen P und irreduciblen Functionen $U(t)$ gelangen wir zu einer Gleichung von der Gestalt

$$f(x, t) = \varphi(x, t)\varphi'(x, t),$$

wo $\varphi(x, t)$ und $\varphi'(x, t)$ ganze rationale Functionen von x und t mit ganzzahligen Coefficienten sind. Diese Gleichung sagt aus, dass die ursprünglich vorgelegte Function $f(x, t)$ reducibel ist. Da aber diese Folgerung mit der Voraussetzung unseres Theorems in Widerspruch steht, so ist unsere anfangs gemachte Annahme unzulässig, d. h. es giebt keine Grenze C derart, dass die vorgelegte Function $f(x, t)$ für alle diese Grenze C überschreitenden ganzzahligen Werthe von t reducibel wird, und damit ist der Beweis unseres Theorems vollständig erbracht.

Der Kürze wegen habe ich die ganze Untersuchung so geführt, dass dieselbe nur die Existenz einer Zahl t von der im Theorem verlangten Beschaffenheit erkennen lässt. Es kann jedoch die Entwicklung ohne Schwierigkeit so ergänzt werden, dass aus derselben zugleich hervorgeht, wie sich eine solche Zahl t mittelst Rechnung durch eine endliche Anzahl von Handlungen wirklich finden lässt, sobald eine bestimmte ganzzahlige Function vorgelegt ist.

Im Folgenden beschäftigen wir uns mit einigen Verallgemeinerungen und Anwendungen des eben bewiesenen Theorems I. Dabei genüge hin-

sichtlich der Beweise der Sätze eine kurze Andeutung der anzuwendenden Schlüsse.

Zunächst nehmen wir an, es seien statt der einen irreduciblen Function $f(x, t)$ mehrere irreducible Functionen $f(x, t)$, $g(x, t)$, $\dots$, $k(x, t)$ vorgelegt. Wir finden dann durch eine leicht erkennbare Abänderung des obigen Schlussverfahrens den folgenden Satz:

Wenn $f(x, t)$, $g(x, t)$, $\dots$, $k(x, t)$ sämtlich ganze ganzzahlige irreducible Functionen der beiden Veränderlichen x und t sind, so ist es stets auf unendlich viele Weisen möglich, für t eine ganze rationale Zahl einzusetzen, so dass dadurch jede dieser Functionen $f(x, t)$, $g(x, t)$, $\dots$, $k(x, t)$ in eine irreducible Function der einen Veränderlichen x übergeht.

Sprechen wir diese Thatsache für das Product $F(x, t)$ der sämtlichen vorgelegten Functionen $f(x, t)$, $g(x, t)$, $\dots$, $k(x, t)$ aus, so ergibt sich der Satz:

In einer beliebig gegebenen ganzen ganzzahligen Function $F(x, t)$ der beiden Veränderlichen x und t lässt sich stets für t auf unendlich viele Weisen eine ganze Zahl derart einsetzen, dass in Bezug auf die Veränderliche x die entstehende Function genau in ebenso viele ganze ganzzahlige irreducible Functionen zerfällt, wie die ursprüngliche Function $F(x, t)$ bei unbestimmtem Parameter t .

Schwieriger ist es, unser Theorem I sowie die eben erwähnten Folgerungen auf den Fall auszudehnen, dass die gegebenen Functionen statt der einen Veränderlichen x beliebig viele Veränderliche $x, y, \dots, w$ und statt des einen Parameters t beliebig viele Parameter $t, r, \dots, q$ enthalten. Um diesen allgemeinsten Fall zu behandeln, beweisen wir zunächst den folgenden Satz:

Wenn $F(x, t, r, \dots, q)$ eine irreducible ganze ganzzahlige Function der Veränderlichen x und der Parameter $t, r, \dots, q$ bezeichnet, so kann man stets für $t, r, \dots, q$ lineare ganze ganzzahlige Functionen eines Parameters u einsetzen, so dass dadurch die Function $F(x, t, r, \dots, q)$ in eine irreducible Function der beiden Veränderlichen x und u übergeht. *)

Es sei

$$F(x, t, r, \dots, q) = f x^n + f_1 x^{n-1} + \dots + f_n,$$

*) Vgl. die von L. Kronecker zu ähnlichem Zwecke angegebene Substitution: Grundzüge einer arithmetischen Theorie der algebraischen Grössen, dieses Journal Bd. 92, S. 11.

$\alpha_y^{(0,0,\dots,0)}$ gleich den ν Wurzeln der Gleichung $\varphi(y) = 0$ und die constanten Glieder der μ letzten Potenzreihen $\gamma_1^{(0,0,\dots,0)}, \dots, \gamma_\mu^{(0,0,\dots,0)}$ sind gleich den μ Wurzeln der Gleichung $\chi(y) = 0$. Wir bilden jetzt die elementarsymmetrischen Functionen der ν ersten Entwicklungen und erhalten dadurch die folgenden ν Potenzreihen

$$\begin{aligned} y_1 + \dots + y_\nu &= \sum A_i^{(\tau, e, \dots, z)} t^{\tau'} r'^e \dots q'^z, \\ . &. \\ y_1 \dots y_\nu &= \sum A'_\nu^{(\tau, e, \dots, z)} t^{\tau'} r'^e \dots q'^z; \\ (\tau, e, \dots, z = 1, 2, 3, \dots) \end{aligned}$$

so fortfahrend bilden wir schliesslich die elementarsymmetrischen Functionen der μ letzten Entwicklungen, wie folgt:

[illegible]

Wir sind somit zu Systemen von Potenzreihen gelangt, von denen das erste System aus ν Potenzreihen und das letzte System aus μ Potenzreihen besteht: die Coefficienten $A, \dots, \Gamma$ dieser Potenzreihen sind rationale Zahlen, und es brechen jedenfalls die Potenzreihen eines Systems nicht sämmtlich im Endlichen ab; denn dieser Umstand hätte, wie man leicht zeigt, die Reducibilität der Function $G(y, t, r, \dots, q)$ zur Folge. Wir combiniren nunmehr noch die verschiedenen Systeme von Potenzentwickelungen unter einander, z. B. die Entwickelungen $y_1, \dots, y_\nu$ und $y_{n-\mu+1}, \dots, y_n$, und stellen dann auch für diese combinirten Systeme die elementarsymmetrischen Functionen auf, so dass wir schliesslich zu einer jeden irreduciblen oder reduciblen in $G(y, t_0, r_0, \dots, q_0)$ aufgehenden ganzzahligen Function je ein System von Potenzreihen mit folgenden Eigenschaften erhalten: die Coefficienten der Potenzreihen sind rationale Zahlen, und es brechen jedenfalls die Potenzreihen eines Systems nicht sämmtlich im Endlichen ab.

Nachdem dies geschehen ist, setzen wir

$$t' = t_1 u, \quad r' = r_1 u, \quad \dots, \quad q' = q_1 u$$

und verwandeln dadurch unsere Potenzreihen in Potenzreihen der einen Veränderlichen u : es ist dann unsere Aufgabe zu zeigen, dass man stets für $t_1, r_1, \dots, q_1$ ganze rationale Zahlen so wählen kann, dass auch nach dieser Substitution die Potenzreihen eines Systems nicht sämtlich im Endlichen abbrechen. Um diesen Beweis zu führen, bezeichnen wir mit E

eine Zahl, welche grösser ist als die Summe der Exponenten der höchsten Potenzen von $t, r, \dots, q$, welche in dem Ausdruck $G(y, t, r, \dots, q)$ vorkommen. Es sei ferner $A t^{\tau_a} r^{\varrho_a} \dots q^{\kappa_a}$ ein solches Glied in einer dem ersten System angehörigen Potenzreihe, für welches der Coefficient A von Null verschieden ist und ausserdem die Exponentensumme $\tau_a + \varrho_a + \dots + \kappa_a$ die Zahl E übertrifft; wir wählen auch in jedem der übrigen Systeme von Potenzreihen ein Glied von der nämlichen Beschaffenheit aus, und es sei etwa $\Gamma t^{\tau_\gamma} r^{\varrho_\gamma} \dots q^{\kappa_\gamma}$ ein Glied in dem zum Factor χ gehörigen Systeme, dessen Coefficient Γ von Null verschieden und wo $\tau_\gamma + \varrho_\gamma + \dots + \kappa_\gamma$ grösser als die Zahl E ist. Wie eine einfache Ueberlegung zeigt, kann man für $t_1, r_1, \dots, q_1$ ganze rationale Zahlen derart wählen, dass in den so entstehenden Potenzreihen der Veränderlichen u beziehentlich die mit

$$u^{\tau_a + \varrho_a + \dots + \kappa_a}, \quad \dots, \quad u^{\tau_\gamma + \varrho_\gamma + \dots + \kappa_\gamma}, \quad \dots$$

multiplicirten Glieder Coefficienten haben, welche von Null verschieden sind. Hieraus folgt aber, dass die einem und dem nämlichen System angehörigen Potenzreihen für die Veränderliche u nicht sämmtlich im Endlichen abbrechen können; denn wäre dies der Fall, so müsste nothwendig die Function $G(y, t, r, \dots, q)$ nach Einführung der Werthe

$$t = t_1 u + t_0, \quad r = r_1 u + r_0, \quad \dots, \quad q = q_1 u + q_0$$

in eine Function von y und u übergehen, welche in zwei oder mehr ganze ganzzahlige Factoren zerfällt. Es würde aber dieser Umstand seinerseits erfordern, dass in den sämmtlichen dem Systeme angehörigen Potenzreihen die Coefficienten aller derjenigen Glieder verschwinden, für welche der Exponent der Potenz von u die Zahl E überschreitet, und letzteres ist thatsächlich nicht der Fall. Damit haben wir bewiesen, dass auch nach Ausführung jener Substitution die Potenzreihen eines Systems nicht sämmtlich im Endlichen abbrechen, und hieraus wiederum folgt, dass die aus $G(y, t, r, \dots, q)$ vermöge jener Substitution entstehende Function der beiden Veränderlichen y und u nothwendig irreducibel ist. Wenn wir jetzt in der ursprünglich vorgelegten Function $F(x, t, r, \dots, q)$ jene Substitution ausführen, so folgt, dass die entstehende Function der beiden Veränderlichen x und u jedenfalls nicht in mehrere von x abhängige Factoren zerfallen kann. Es bliebe mithin nur noch die Möglichkeit übrig, dass die aus $F(x, t, r, \dots, q)$ vermöge jener Substitution entstehende Function einen Factor besitzt, welcher allein die Veränderliche u enthält. Man kann aber, wie ersichtlich ist, die

ganzen Zahlen $t_1, r_1, \dots, q_1$ zugleich so wählen, dass auch dieser Fall nicht eintritt. Damit ist der Beweis für den vorhin ausgesprochenen Satz vollständig erbracht. Mit Hilfe dieses Satzes beweisen wir jetzt das folgende allgemeine Theorem:

II. Wenn $F(x, y, \dots, w; t, r, \dots, q)$ eine irreducible ganze ganzzahlige Function der Veränderlichen $x, y, \dots, w$ und der Parameter $t, r, \dots, q$ bezeichnet, so ist es stets auf unendlich viele Weisen möglich, für die Parameter $t, r, \dots, q$ ganze rationale Zahlen einzusetzen, so dass dadurch die Function $F(x, y, \dots, w; t, r, \dots, q)$ in eine irreducible Function der Veränderlichen $x, y, \dots, w$ übergeht.

Wenn wir in der vorgelegten Function $F(x, y, \dots, w; t, r, \dots, q)$ die Substitution

$$y = \eta x, \quad \dots, \quad w = \omega x$$

vornehmen und dann die etwa als gemeinsamer Factor auftretende Potenz von x fortlassen, so entsteht eine Function $G(x, \eta, \dots, \omega, t, r, \dots, q)$ der Veränderlichen x und der Parameter $\eta, \dots, \omega, t, r, \dots, q$, welche ebenfalls irreducibel ist. Wir setzen zunächst nach dem eben bewiesenen Satze für diese Parameter lineare ganzzahlige Functionen eines einzigen Parameters u ein, nämlich

$$\begin{aligned} \eta &= \eta_1 u + \eta_0, & \dots, & & \omega &= \omega_1 u + \omega_0, \\ t &= t_1 u + t_0, & \dots, & & q &= q_1 u + q_0, \end{aligned}$$

so dass jene Function übergeht in eine irreducible Function $g(x, u)$ der beiden Veränderlichen x und u . Es lässt sich dann nach unserem Theoreme I. für u eine ganze rationale Zahl u_0 einsetzen, so dass die Function $g(x, u_0)$ eine irreducible Function der einen Veränderlichen x wird. Nunmehr erkennen wir, dass die ursprünglich vorgelegte Function $F(x, y, \dots, w; t, r, \dots, q)$ nothwendig in eine irreducible Function der Veränderlichen $x, y, \dots, w$ übergeht, wenn wir für die Parameter die ganzen Zahlen

$$t = t_1 u_0 + t_0, \quad r = r_1 u_0 + r_0, \quad \dots, \quad q = q_1 u_0 + q_0$$

einsetzen; denn die so entstehende Function würde in eine irreducible Function der einen Veränderlichen x übergehen, wenn wir überdies noch setzen:

$$y = (\eta_1 u_0 + \eta_0)x, \quad \dots, \quad w = (\omega_1 u_0 + \omega_0)x$$

und von einer etwa als Factor auftretenden Potenz der Veränderlichen x absehen. Damit ist der verlangte Nachweis geführt.

Wir haben bisher in allen unseren Entwicklungen und Betrachtungen über die Irreducibilität stets den Bereich der rationalen Zahlen zu Grunde gelegt: eine ganze Function wurde dann kurzweg irreducibel genannt, wenn sie sich nicht als Product von mehreren ganzen Functionen mit ganzzahligen rationalen Coefficienten darstellen liess. Es ist jetzt nothwendig, die gefundenen Sätze auf den Fall eines beliebigen durch eine algebraische Zahl bestimmten Rationalitätsbereiches auszudehnen. Wir nennen dementsprechend, wie es üblich ist, eine ganze rationale Function, deren Coefficienten einem gegebenen durch eine algebraische Zahl bestimmten Rationalitätsbereiche angehören, irreducibel in diesem Bereiche, wenn sie nicht als Product von mehreren ganzen rationalen Functionen dargestellt werden kann, deren Coefficienten in eben jenem Rationalitätsbereiche liegen. Es gilt dann das folgende Theorem:

III. *Wenn die Function $F(x, y, \dots, w; t, r, \dots, q)$ in einem gewissen durch eine algebraische Zahl bestimmten Rationalitätsbereiche irreducibel ist, so ist es stets auf unendlich viele Weisen möglich, in dieser Function $F(x, y, \dots, w; t, r, \dots, q)$ für die Parameter $t, r, \dots, q$ ganze rationale Zahlen einzusetzen, so dass dadurch diese Function in eine Function der Veränderlichen $x, y, \dots, w$ übergeht, welche in eben jenem Rationalitätsbereiche irreducibel ist.*

Das eben ausgesprochene Theorem III. lässt sich auf das Theorem II. zurückführen, und zwar mit Hülfe eines Verfahrens, welches L. Kronecker*) anwendet, um in einem beliebigen Rationalitätsbereiche die Zerlegung einer ganzen rationalen Function in ihre irreducibeln Factoren zu bewirken. Wir sorgen nöthigenfalls zunächst durch Multiplication mit einer Zahl des gegebenen Bereiches und durch geeignete Transformation der Veränderlichen dafür, dass die Function F mindestens ein Glied mit einem ganzen rationalen Coefficienten enthält, und dass ausserdem alle zu F conjugirten Functionen von einander verschieden sind. Wir bilden das Product dieser sämtlichen conjugirten Functionen und erhalten dann nach Multiplication mit einer geeigneten ganzen rationalen Zahl eine ganze rationale Function G von $x, y, \dots, w, t, r, \dots, q$ mit ganzen rationalen Coefficienten, welche im Bereiche der rationalen Zahlen irreducibel ist. Es lassen sich daher

*) Vgl. Grundzüge einer arithmetischen Theorie der algebraischen Grössen, dieses Journal Bd. 92 S. 12 und 13.

zufolge des Theorems II. für $t, r, \dots, q$ ganze rationale Zahlen so bestimmen, dass nach deren Einsetzung G in eine Function der Veränderlichen $x, y, \dots, w$ übergeht, welche im Bereiche der rationalen Zahlen irreducibel ist. Wie leicht gezeigt werden kann, geht dann die ursprünglich vorgelegte Function $F(x, y, \dots, w; t, r, \dots, q)$ nach Einsetzung der nämlichen ganzzahligen Werthe für $t, r, \dots, q$ in eine Function der Veränderlichen $x, y, \dots, w$ über, welche in dem gegebenen durch jene algebraische Zahl bestimmten Rationalitätsbereiche irreducibel ist.

Wir wenden nun die gewonnenen Resultate auf die Theorie der Gleichungen an. Es sei eine Gleichung n ten Grades in x vorgelegt von der Gestalt

$$F_0 x^n + F_1 x^{n-1} + \dots + F_n = 0,$$

deren Coefficienten $F_0, F_1, \dots, F_n$ ganze rationale Functionen der Parameter $t, r, \dots, q$ mit ganzen rationalen Zahlencoefficienten sind. Um die Gruppe Γ der Gleichung in dem durch die rationalen Zahlen und die Parameter $t, r, \dots, q$ bestimmten Rationalitätsbereiche zu finden, bilden wir das über alle Permutationen $i_1, i_2, \dots, i_n$ der n Zahlen $1, 2, \dots, n$ erstreckte Product:

$$\Pi(u + x_{i_1} u_1 + x_{i_2} u_2 + \dots + x_{i_n} u_n),$$

wo $u, u_1, u_2, \dots, u_n$ unbestimmte Parameter und $x_1, x_2, \dots, x_n$ die n Wurzeln der Gleichung bedeuten. Dieses Product Π wird nach Multiplication mit F_0^n eine ganze ganzzahlige Function der Unbestimmten $u, u_1, u_2, \dots, u_n, t, r, \dots, q$, und wenn $G(u, u_1, \dots, u_n, t, r, \dots, q)$ ein ganzer ganzzahliger im Bereiche der rationalen Zahlen irreducibler Factor dieser Function ist, so wird die gesuchte Gruppe Γ durch diejenigen Permutationen bestimmt, welche die Function G ungeändert lassen. Wie wir jetzt mit Hülfe der obigen Entwicklungen zeigen wollen, kann man in die vorgelegte Gleichung auf unendlich viele Weisen für die Parameter $t, r, \dots, q$ ganze rationale Zahlen derart einsetzen, dass die so entstehende ganzzahlige Gleichung im Bereiche der rationalen Zahlen die nämliche Gruppe Γ besitzt. Um dies zu beweisen, berechnen wir die Discriminante D der vorgelegten Gleichung; dieselbe wird nach Multiplication mit einer Potenz von F_0 eine ganze ganzzahlige nicht identisch verschwindende Function der Parameter $t, r, \dots, q$. Wir können dann nach Theorem II. zunächst für t unbegrenzt viele ganze rationale Zahlen bestimmen, nach deren Einsetzung G eine im

Bereich der rationalen Zahlen irreducible Function der Veränderlichen u , $u_1, \dots, u_n, r, \dots, q$ wird. Unter diesen ganzen rationalen Zahlen t wählen wir eine solche aus, für welche D nicht identisch verschwindet. Hierauf bestimmen wir eine ganze rationale Zahl r , bei deren Einsetzung die Function G eine im Bereiche der rationalen Zahlen irreducible Function der übrig bleibenden Veränderlichen wird, und für welche überdies die Discriminante D von Null verschieden bleibt. So fortfahrend erhalten wir für $t, r, \dots, q$ ganze rationale Zahlen, nach deren Einsetzung G in eine ganze ganzzahlige irreducible Function g der Unbestimmten $u, u_1, \dots, u_n$ übergeht, und für welche die Discriminante D der Gleichung eine von Null verschiedene rationale Zahl wird. Es ist nun einerseits offenbar, dass alle Substitutionen, welche G zulässt, auch die Function g nicht ändern können, und andererseits kann die Function g ausser diesen Substitutionen nicht noch andere Substitutionen zulassen, da die Ordnung der Gruppe für die entstehende ganzzahlige Gleichung jedenfalls nicht grösser als die Ordnung der Gruppe Γ sein kann: Γ ist mithin zugleich die Gruppe der durch Einsetzung jener ganzen Zahlen entstehenden ganzzahligen Gleichung.

Nehmen wir beispielsweise in einer Gleichung die Coefficienten selber als die unbestimmten Parameter $t, r, \dots, q$ an, so ist die Gruppe Γ der Gleichung die symmetrische, und es folgt daher, *dass es unbegrenzt viele Gleichungen n ten Grades mit ganzzahligen Coefficienten giebt, deren Gruppe im Bereiche der rationalen Zahlen die symmetrische Gruppe ist.*

Zu solchen Gleichungen kann man im Allgemeinen sogar gelangen, wenn man sich lediglich die geeignete Wahl des letzten Coefficienten in der Gleichung vorbehält. Um dies einzusehen, nehmen wir in der Gleichung

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + t = 0$$

die Coefficienten $a_0, a_1, \dots, a_{n-1}$ als ganze rationale Zahlen irgendwie an mit der Einschränkung, dass die Gleichung

$$f'(x) = n a_0 x^{n-1} + (n-1) a_1 x^{n-2} + \dots + a_{n-1} = 0$$

lauter verschiedene Wurzeln besitzt und die Function $f(x)$ für diese Wurzeln lauter verschiedene Werthe annimmt. Die Discriminante der ersteren Gleichung wird dann eine ganze rationale Function $(n-1)$ ten Grades in t , welche lauter verschiedene Linearfactoren besitzt. Aus diesem Umstande kann mit Hülfe derjenigen Principien, welche Herr A. Hurwitz*) dargelegt hat, gefolgert werden,

*) Mathematische Annalen Bd. 39 S. 1.

dass die Monodromiegruppe jener Gleichung bezüglich des Parameters t die symmetrische ist*). Aus dem vorhin bewiesenen allgemeinen Satze ergibt sich sodann, dass man in unserer Gleichung auf unendlich viele Weisen für den letzten Coefficienten t eine ganze Zahl derart einsetzen kann, dass die entstehende ganzzahlige Gleichung im Bereich der rationalen Zahlen die symmetrische Gruppe besitzt.

Durch ähnliche Schlüsse sind wir im Stande zu zeigen, dass es unbegrenzt viele Gleichungen mit ganzen rationalen Zahlencoefficienten giebt, deren Gruppe im Bereiche der rationalen Zahlen die alternirende Gruppe ist. Zum Beweise brauchen wir einige Sätze, deren Richtigkeit man ohne Schwierigkeit mittelst derjenigen Methoden erkennen kann, welche Herr A. Hurwitz in den vorhin angeführten Arbeiten auseinandersetzt. Der erste dieser Sätze lautet, wie folgt:

Es sei $f(x)$ eine ganze rationale Function der Veränderlichen x vom geraden Grade n , welche den Factor x^2 besitzt, und der Differentialquotient dieser Function habe die Gestalt

$$f'(x) = nx(x-a)^2(x-b)^2 \dots (x-k)^2;$$

dabei seien $a, b, \dots, k$ von Null und unter einander verschiedene Grössen, und auch die Werthe $f(a), f(b), \dots, f(k)$ seien unter einander verschieden: dann ist die Monodromiegruppe der Gleichung

$$f(x) + t^2 = 0$$

bezüglich des Parameters t gleich der alternirenden Gruppe.

Wir berechnen zunächst die Discriminante dieser Gleichung, indem wir uns dabei einer bekannten Formel für die Resultante zweier ganzen Functionen bedienen. Wenn nämlich $\varphi(x)$ und $\psi(x)$ zwei ganze rationale Functionen der Veränderlichen x vom Grade ν und μ und mit den Nullstellen $\alpha_1, \alpha_2, \dots, \alpha_\nu$ und $\beta_1, \beta_2, \dots, \beta_\mu$ bedeuten, und wenn wir dementsprechend

$$\varphi(x) = \alpha(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_\nu),$$

$$\psi(x) = \beta(x - \beta_1)(x - \beta_2) \dots (x - \beta_\mu)$$

setzen, so gilt die Formel

$$\begin{aligned} R(\varphi, \psi) &= \beta^\nu \varphi(\beta_1) \varphi(\beta_2) \dots \varphi(\beta_\mu) \\ &= (-1)^{\nu\mu} \alpha^\mu \psi(\alpha_1) \psi(\alpha_2) \dots \psi(\alpha_\nu). \end{aligned}$$

*) Vgl. ausserdem A. Hurwitz: Ueber diejenigen algebraischen Gebilde, welche eindeutige Transformationen in sich zulassen. Nachrichten der Kgl. Gesellschaft der Wissenschaften zu Göttingen, 1887 S. 103, wo die oben von mir benutzte Thatsache ebenfalls zur Geltung kommt.

Mit Hülfe derselben finden wir für die Discriminante der obigen Gleichung, d. h. für das Product der quadrierten Wurzeldifferenzen, den Werth

$$D = n^n t^2 (f(a) + t^2)^2 (f(b) + t^2)^2 \dots (f(k) + t^2)^2,$$

und das Product der Wurzeldifferenzen selbst wird daher

$$D^{\frac{1}{2}} = n^{\frac{n}{2}} t (f(a) + t^2) (f(b) + t^2) \dots (f(k) + t^2).$$

Wir setzen jetzt für $a, b, \dots, k$ irgend welche rationalen positiven und von einander verschiedenen Zahlen. Nach Annahme dieser Zahlen ist $f(x)$ völlig bestimmt, und auch die Werthe $f(a), f(b), \dots, f(k)$ sind unter einander sämmtlich verschieden; denn es ist beispielsweise $f(b) - f(a)$ gleich dem von a bis b erstreckten Integrale über die in diesem Intervalle nirgends negative Function $f'(x)$. Da n eine gerade Zahl ist, so ist der gefundene Ausdruck für $D^{\frac{1}{2}}$ eine ganze rationale Function von t mit rationalen Zahlencoefficienten, und folglich ist auch die Gruppe der Gleichung in dem durch die rationalen Zahlen und den Parameter t bestimmten Bereiche gleich der alternirenden Gruppe. Man kann jetzt nach dem oben bewiesenen allgemeinen Satze auf unendlich viele Weisen für t eine ganze Zahl einsetzen, so dass die entstehende ganzzahlige Gleichung im Bereiche der rationalen Zahlen die alternirende Gruppe besitzt, und damit ist unsere Behauptung für Gleichungen geraden Grades bewiesen.

Um die entsprechende Thatsache für Gleichungen vom ungeraden Grade n einzusehen, benutzen wir einen Satz, welcher wiederum ohne Schwierigkeit aus den von Herrn A. Hurwitz entwickelten Principien gefolgert werden kann. Dieser Satz lautet:

Es sei $f(x)$ eine ganze rationale Function der Veränderlichen x vom ungeraden Grade n , welche mit ihrem Differentialquotienten $f'(x)$ durch die Formel

$$xf'(x) - f(x) = (n-1)(x-a)(x-b)^2(x-c)^2 \dots (x-k)^2$$

verbunden ist; dabei seien $a, b, c, \dots, k$ von Null und unter einander verschiedene Grössen, und auch die Werthe $f'(b), f'(c), \dots, f'(k)$ seien von einander verschieden: dann ist die Monodromiegruppe der Gleichung

$$f(x) + (t^2 - f'(a))x = 0$$

bezüglich des Parameters t gleich der alternirenden Gruppe.

Indem wir uns der oben angegebenen Formel für die Resultante zweier ganzen Functionen und ausserdem der Formel

$$R(\varphi - x\psi, \psi) = R(\varphi, \psi)$$

bedienen, finden wir für die Discriminante jener Gleichung, d. h. für das Product der quadrirten Wurzeldifferenzen, den Werth

$$D = (n-1)^{n-1} t^2 (t^2 + f'(b) - f'(a))^2 (t^2 + f'(c) - f'(a))^2 \dots (t^2 + f'(k) - f'(a))^2,$$

und das Product der Wurzeldifferenzen selbst wird daher

$$D^{\frac{1}{2}} = (n-1)^{\frac{n-1}{2}} t (t^2 + f'(b) - f'(a)) (t^2 + f'(c) - f'(a)) \dots (t^2 + f'(k) - f'(a)).$$

Wir wählen jetzt für $b, c, \dots, k$ irgend welche rationalen positiven und von einander verschiedenen Zahlen und setzen

$$a = -\frac{1}{2\left(\frac{1}{b} + \frac{1}{c} + \dots + \frac{1}{k}\right)}.$$

In Folge der letzteren Annahme verschwindet auf der rechten Seite der Formel

$$xf'(x) - f(x) = (n-1)(x-a)(x-b)^2(x-c)^2 \dots (x-k)^2$$

der Coefficient von x , gerade wie dies auf der linken Seite der Fall ist, und es lässt sich deswegen eine ganze rationale Function $f(x)$ vom n ten Grade mit rationalen Zahlencoefficienten bestimmen, welche dieser Formel genügt. Diese Function $f(x)$ besitzt zugleich die Eigenschaft, dass die Werthe $f'(b), f'(c), \dots, f'(k)$ sämmtlich von einander verschieden sind; denn es ist beispielsweise

$$f'(c) - f'(b) = \frac{f(c)}{c} - \frac{f(b)}{b} = \int_b^c \frac{xf'(x) - f(x)}{x^2} dx,$$

und hierin wird die unter dem Integralzeichen stehende Function zwischen den Integrationsgrenzen nirgends negativ. Da n eine ungerade Zahl ist, so ist der gefundene Ausdruck für $D^{\frac{1}{2}}$ eine ganze rationale Function von t mit rationalen Zahlencoefficienten, und folglich ist auch die Gruppe der Gleichung in dem durch die rationalen Zahlen und den Parameter t bestimmten Bereiche gleich der alternirenden Gruppe. Man kann jetzt nach dem oben bewiesenen allgemeinen Satze auf unendlich viele Weisen für t eine ganze Zahl einsetzen, so dass die entstehende ganzzahlige Gleichung im Bereiche der rationalen Zahlen die alternirende Gruppe besitzt, und damit ist unsere Behauptung auch für Gleichungen ungeraden Grades bewiesen.

Mit Hülfe des Theorems III. lassen sich die bisher über die Gruppe einer Gleichung angestellten Betrachtungen auf beliebige durch eine algebraische Zahl bestimmte Rationalitätsbereiche ausdehnen. Wir gelangen so durch die entsprechenden Schlüsse zu dem folgenden Satze:

IV. *Es sei eine algebraische Zahl $\Re$ und ausserdem eine Gleichung n ten Grades von der Gestalt*

$$F_0 x^n + F_1 x^{n-1} + \dots + F_n = 0$$

gegeben; die Coefficienten $F_0, F_1, \dots, F_n$ seien ganze rationale Functionen der Parameter $t, r, \dots, q$, deren Coefficienten Zahlen des durch $\Re$ bestimmten Rationalitätsbereiches sind. Ist dann Γ die Gruppe der Gleichung in dem durch die algebraische Zahl $\Re$ und durch die Parameter $t, r, \dots, q$ bestimmten Rationalitätsbereiche, so lassen sich stets auf unendlich viele Weisen für die Parameter $t, r, \dots, q$ ganze rationale Zahlen einsetzen derart, dass die so entstehende numerische Gleichung in dem durch die algebraische Zahl $\Re$ bestimmten Rationalitätsbereiche eben jene Gruppe Γ besitzt.

Dieser Satz bietet ein principiellcs Interesse, indem er zeigt, dass die formal in den Coefficienten der Gleichung und im Rationalitätsbereiche auftretenden Parameter stets durch ganze rationale Zahlen ersetzt werden können, sobald es sich lediglich um die gruppentheoretischen Eigenschaften der Gleichung handelt: man vermeidet also auf diesem Wege die Adjunction algebraischer Functionen.

Um zu zeigen, wie sich mit den gewonnenen Mitteln der Begriff der Monodromiegruppe in arithmetischer Weise erklären lässt, nehmen wir an, es sei eine Gleichung gegeben, deren Coefficienten ganze rationale Functionen des einen Parameters t sind, und die Coefficienten dieser ganzen rationalen Functionen seien Zahlen eines durch die Zahl $\Re$ bestimmten Rationalitätsbereiches. Wir setzen jetzt für t irgend eine ganze rationale Zahl ein und denken uns die Gruppen aller so entstehenden numerischen Gleichungen in dem durch $\Re$ bestimmten Rationalitätsbereiche aufgestellt. Es sei ferner $\mathfrak{A}$ eine algebraische Zahl, durch deren Adjunction die Gruppen jener Gleichungen sämtlich eine Verkleinerung erleiden, und es gebe nun keine Zahl mehr, bei deren Adjunction eine weitere Verkleinerung sämtlicher Gruppen eintritt. Diejenige von den verkleinerten Gruppen, welche die grösste Ordnung besitzt, stimmt überein mit der Monodromiegruppe der ursprünglich gegebenen Gleichung bezüglich des Parameters t .

Auf Grund des Theorems IV. können wir auch unsere früheren Sätze über die symmetrische und alternirende Gruppe verallgemeinern; wir finden dann folgende Thatfachen: *wenn ein beliebiger durch eine algebraische Zahl bestimmter Rationalitätsbereich gegeben ist, so kann man stets Gleichungen mit rationalen Zahlencoefficienten angeben, deren Gruppe in jenem Rationalitäts-*

bereiche die symmetrische und ebenso solche, deren Gruppe in jenem Rationalitätsbereiche die alternirende ist. Es giebt also auch in jedem durch eine algebraische Zahl bestimmten Rationalitätsbereiche Gleichungen von beliebigem die Zahl vier übersteigendem Grade n mit rationalen Zahlen-coefficienten, welche in jenem Bereiche durch Wurzelziehen nicht lösbar sind.

Ebenso zeigt man leicht, *dass es unbegrenzt viele von einander verschiedene Bereiche von bestimmtem Grade n* (Gattungsbereiche n ter Ordnung, Zahlenkörper n ten Grades) *giebt, in denen — abgesehen vom Bereiche aller rationalen Zahlen — kein Bereich niederen Grades enthalten ist.* Gäbe es nämlich nur eine endliche Anzahl solcher Bereiche, so vereinigen wir diese zu einem neuen Rationalitätsbereiche $\mathfrak{R}$. Nach den obigen Entwicklungen giebt es dann eine Gleichung n ten Grades mit rationalen Coefficienten, welche im Bereiche $\mathfrak{R}$ die symmetrische Gruppe besitzt. Diese Gleichung definirt dann offenbar einen Bereich n ten Grades, welcher von den eben angenommenen Bereichen n ten Grades verschieden ist und überdies keinen Bereich niederen Grades enthält. Entsprechend beweisen wir die allgemeinere Thatsache, dass es unbegrenzt viele Bereiche vom Grade $n = \nu\mu$ giebt, welche einen gegebenen Bereich ν ten Grades und — vom Bereiche aller rationalen Zahlen abgesehen — nur diesen enthalten.

In der vorstehenden Untersuchung ist lediglich die Existenz der Gleichungen und Bereiche von gewissen Eigenschaften behauptet und bewiesen worden. Es kann jedoch entsprechend dem oben bei Ableitung des Theorems I. hervorgehobenen Umstände die Entwicklung so ergänzt werden, dass aus derselben zugleich hervorgeht, wie sich jene Gleichungen und Bereiche wirklich durch Rechnung aufstellen lassen.

Zum Schluss erwähne ich noch einen Satz, welcher sich ebenfalls mit den oben benutzten Hilfsmitteln erledigen lässt, aber auch direct durch geeignete Anwendung von Potenzentwicklungen bewiesen werden kann. Dieser Satz lautet: Wenn eine algebraische Function von t für alle rationalen in einem beliebig kleinen Intervalle gelegenen Werthe stets selber rationale Werthe annimmt, so ist sie nothwendig eine rationale Function*).

*) Eine analytische Function kann sehr wohl für alle rationalen Argumente rationale Werthe annehmen, wie dies neuerdings von E. Strauss gezeigt worden ist.