ÜBER
EINIGE ANWENDUNGEN DER MODULSYSTEME AUF ELEMENTARE ALGEBRAISCHE FRAGEN.

VON

L. KRONECKER.

Crelle, Journal für die reine und angewandte Mathematik. Band 99. S. 329—371.

ÜBER EINIGE ANWENDUNGEN DER MODULSYSTEME AUF ELEMENTARE ALGEBRAISCHE FRAGEN.

I.

Einleitende Bemerkungen über Congruenzen nach Modulsystemen.

Durch den *Congruenzbegriff*, welchen *Gauss* im art. I der „*Disquisitiones arithmeticae*“ eingeführt hat, wird von dem speciellen Werthe des ganzzahligen Coefficienten von m in der Zahlform*):

$$a + km$$

abstrahirt; es wird das „Gemeinsame“ aller durch diese Zahlform darstellbaren ganzen Zahlen:

$$\ldots, a - 3m, \quad a - 2m, \quad a - m, \quad a, \quad a + m, \quad a + 2m, \quad a + 3m, \ldots$$

hervorgehoben, indem sie als einander „nach dem Modul m congruent“ bezeichnet werden.

Die Reihe der Zahlen $a + km$ ist durch zwei Grössen, nämlich durch den festen Modul m und irgend ein Glied der Reihe, völlig bestimmt; und

*) Vgl. art. II der „*Disquisitiones arithmeticae*“.

es ist demgemäss jede Reihe unter einander (nach irgend einem Modul) congruenter Zahlen:

$$a',\ a'',\ a''',\ \ldots,$$

durch zwei Invarianten zu charakterisiren. Solche zwei Invarianten kann man z. B. (rein arithmetisch) bestimmen, indem man die eine als die ihrem absoluten Werthe nach kleinste der Zahlen a selbst, die andere aber als die absolut kleinste der *Differenzen* der verschiedenen Zahlen a definirt.*) Die letztere Invariante giebt dann den absoluten Werth des Moduls m, nach welchem die verschiedenen Zahlen der Reihe a', a'', a''', ... einander congruent sind, während die erstere den Werth:

$$mR\left(\frac{a}{m}\right)$$

hat. Hier ist, wie in meinen früheren Aufsätzen, unter $R(a)$ der Rest zu verstehen, welcher verbleibt, wenn man von der Grösse a die ihr zunächst benachbarte Zahl subtrahirt, während für den Fall, wo a genau in der Mitte zwischen zwei benachbarten ganzen Zahlen liegt, $R(a) = -\frac{1}{2}$ zu nehmen ist.

Der ebenso einfache als weittragende Gedanke, welcher der *Gauss*'schen Einführung des Congruenzbegriffes in der ersten Section des *Disqq. arithm.* zu Grunde liegt, lässt sich auch im Anschluss an jene allgemeinen Principien erörtern, mittels deren *Gauss* in der fünften Section seines Werkes die Theorie der quadratischen Formen begründet**). Definirt man nämlich, gemäss den a. a. O. entwickelten Principien, zwei lineare Formen je einer Unbestimmten:

*) Um auch in dem Falle, wo der absolut kleinste Werth der positiven Zahlen a gleich dem der negativen ist, eine Bestimmung zu treffen, kann hinzugefügt werden, dass alsdann die *negative* Zahl als Invariante genommen werden soll.

**) Vgl. meine Auseinandersetzungen über das gedanklich Neue der *Gauss*'schen Theorie am Schlusse des § 22 meiner Festschrift zu Herrn *Kummer*'s Doctorjubiläum S. 94 und 95[1]).

[1]) Bd. II S. 355—356 dieser Ausgabe von *L. Kronecker*'s Werken. H.

$$a + bx,\quad a' + b'x'$$

als einander äquivalent, wenn jede in die andere durch eine ganzzahlige Substitution:

$$x = \alpha x' + \beta,\quad x' = \alpha' x + \beta'$$

übergeführt werden kann, so sind die nothwendigen und hinreichenden Aequivalenzbedingungen die folgenden:

$$b = \pm b',\quad a \equiv a' \pmod{b},$$

und der Begriff der Congruenz der Zahlen:

$$a \equiv a' \pmod{m}$$

deckt sich also vollständig mit dem der Aequivalenz der Linearformen:

$$a + mx \backsim a' + mx',$$

wie ich neulich schon bei einer anderen Gelegenheit auseinander gesetzt habe*).

Nimmt man nun an Stelle der Linearformen mit *einer* Unbestimmten solche mit beliebig vielen Unbestimmten:

$$a + m_1 x_1 + m_2 x_2 + \cdots + m_\mu x_\mu$$

und definirt zwei Formen:

$$a + \sum_{h=1}^{h=\mu} m_h x_h,\quad a' + \sum_{k=1}^{k=\nu} m'_k x'_k$$

als einander äquivalent, wenn sie durch ganzzahlige Substitutionen:

*) Vgl. art. I meines Aufsatzes „Die absolut kleinsten Reste reeller Grössen“ im Sitzungsberichte der hiesigen Akademie der Wissenschaften vom 30. April 1885[1]).

[1]) Bd. III S. 114 dieser Ausgabe. H.

$$x_h = c_{h0} + \sum_k c_{hk} x'_k, \quad x'_k = c'_{k0} + \sum_h c'_{kh} x_h \qquad \binom{h=1,2,\dots\mu}{k=1,2,\dots\nu}$$

in einander transformirt werden, so bildet dies einen unmittelbaren und ganz naturgemässen Uebergang von dem *Gauss*'schen Begriffe der „Congruenz nach einem Modul" zu dem allgemeineren Begriffe der „Congruenz nach einem Systeme von Moduln". Denn die nothwendigen und hinreichenden Bedingungen für die Aequivalenz der Formen:

$$a + \sum_{h=1}^{h=\mu} m_h x_h, \quad a' + \sum_{k=1}^{k=\nu} m'_k x_k$$

werden zuvörderst durch die Gleichungen:

$$(A.) \qquad a = a' + \sum_k c'_{k0} m'_k, \quad a' = a + \sum_h c_{h0} m_h, \qquad \binom{h=1,2,\dots\mu}{k=1,2,\dots\nu}$$

$$(B.) \qquad m_h = \sum_k c'_{kh} m'_k, \qquad m'_k = \sum_h c_{hk} m_h$$

ausgedrückt. Man kann aber ferner, nach *Gauss*' Vorgang, von den speciellen Werthen der ganzzahligen Coefficienten c, c' in den Gleichungen (*A.*) und (*B.*) abstrahiren und das „*Gemeinsame*" der durch die Zahlform:

$$a + \sum_{h=1}^{h=\mu} c_{h0} m_h$$

darstellbaren Zahlen hervorheben, indem man dieselben als einander

„nach dem Modulsystem $(m_1, m_2, \dots m_\mu)$ congruent"

bezeichnet. Dann ergiebt sich auch der Begriff der „Aequivalenz der Modulsysteme"

$$(m_1, m_2, \dots m_\mu), \qquad (m'_1, m'_2, \dots m'_\nu)$$

von selbst, da vermöge der Gleichungen (*B.*) die Gesammtheit der durch jede der beiden Zahlformen:

$$a + \sum_{h=1}^{h=\mu} c_{h0} m_h, \qquad a' + \sum_{k=1}^{k=\nu} c'_{k0} m'_k$$

dargestellten Zahlen genau dieselbe ist, und die Gleichungen (*B.*) erweisen sich demgemäss als *charakteristisch* für die Aequivalenz:

$$(m_1, m_2, \dots m_\mu) \sim (m'_1, m'_2, \dots m'_\nu).$$

Hiernach lassen sich — im unmittelbaren Anschluss an die *Gauss*'schen Entwickelungen — die nothwendigen und hinreichenden Bedingungen für die Aequivalenz der Linearformen:

$$a + \sum_{h=1}^{h=\mu} m_h x_h, \qquad a' + \sum_{k=1}^{k=\nu} m'_k x'_k$$

durch die Congruenz:

$$a \equiv a' \qquad (\text{modd. } m'_1, m'_2, \dots m'_\mu)$$

in Verbindung mit der Aequivalenz:

$$(m_1, m_2, \dots m_\mu) \sim (m'_1, m'_2, \dots m'_\nu)$$

ausdrücken.

Hat das Modulsystem $(m_1, m_2, \dots m_\mu)$, wie hier angenommen worden, lauter ganzzahlige Elemente, so ist es offenbar einem solchen äquivalent, welches nur ein einziges Element, nämlich den grössten gemeinsamen Theiler der μ Zahlen m, enthält. In diesem Falle ist also die Einführung von Modulsystemen unnöthig*). Aber bei dem Fortschritt von der gewöhnlichen Zahlentheorie zur arithmetischen Behandlung ganzzahliger Functionen von unbestimmten Variabeln ist die Einführung von Modulsystemen *nothwendig*.

*) Dass trotzdem die Anwendung von Modulsystemen in der gewöhnlichen Zahlentheorie von mancherlei Nutzen ist, davon habe ich mich in den Universitätsvorlesungen, welche ich in diesem Winter halte, bei mehreren Gelegenheiten überzeugt.

Bedeuten A, M_1, M_2, $\dots M_\mu$, A', M_1', M_2', $\dots M_\nu'$ ganze ganzzahlige Functionen der unbestimmten Variabeln $\mathfrak{R}'$, $\mathfrak{R}''$, $\dots \mathfrak{R}^{(n-2)}$ oder also „ganze Grössen“ des Rationalitätsbereiches $(\mathfrak{R}', \mathfrak{R}'', \dots \mathfrak{R}^{(n-1)})$, so ist gemäss den oben aus dem *Gauss*'schen Congruenzbegriff hergeleiteten Begriffsbestimmungen die Aequivalenz zweier „Modulsysteme“

$$(M_1, M_2, \dots M_\mu), \qquad (M_1', M_2', \dots M_\nu')$$

und die „Congruenz zweier Grössen A, A' nach einem dieser Modulsysteme“ durch ein System von Gleichungen:

$$(\overline{A}.) \qquad A = A' + \sum_k C_{k0}' M_k', \qquad A' = A + \sum_k C_{k0} M_k,$$

$$(\overline{B}.) \qquad M_k = \sum_k C_{kk}' M_k', \qquad M_k' = \sum_k C_{kk} M_k, \qquad \begin{pmatrix} k=1, 2, \dots \mu \\ k=1, 2, \dots \nu \end{pmatrix}$$

zu definiren, in welchen die Coefficienten C, C' ebenfalls ganze Grössen des Rationalitätsbereichs $(\mathfrak{R}', \mathfrak{R}'', \dots \mathfrak{R}^{(n-1)})$ bedeuten. Durch eben dasselbe System von Gleichungen ist aber auch die Aequivalenz der Linearformen:

$$A + \sum_{k=1}^{k=\mu} M_k X_k, \qquad A' + \sum_{k=1}^{k=\nu} M_k' X_k'$$

zu definiren, da diese vermöge der Gleichungen $(\overline{A}.)$ und $(\overline{B}.)$ in einander durch Substitutionen mit *ganzen*, dem Rationalitätsbereich $(\mathfrak{R}', \mathfrak{R}'', \dots \mathfrak{R}^{(n-1)})$ angehörigen Coefficienten übergehen. Die Aequivalenz dieser beiden Linearformen wird also wiederum durch die „Congruenz“:

$$A \equiv A' \pmod{M_1, M_2, \dots M_\mu}$$

in Verbindung mit der „Aequivalenz“:

$$(M_1, M_2, \dots M_\mu) \sim (M_1', M_2', \dots M_\nu')$$

charakterisirt.

Wenn die Linearform $M_1 X_1 + M_2 X_2 + \cdots + M_\mu X_\mu$ durch lineare Substitution mit ganzen, dem Rationalitätsbereich $(\mathfrak{R}', \mathfrak{R}'', \dots \mathfrak{R}^{(n-1)})$ angehörigen Coefficienten in die Linearform $M_1' X_1' + M_2' X_2' + \cdots + M_\nu' X_\nu'$ übergeht, so ist nach Analogie der von *Gauss* in die Theorie der quadratischen Formen eingeführten Begriffsbestimmungen die erstere Linearform als „die letztere enthaltend“ zu bezeichnen. Wird diese Ausdrucksweise auf die *Coefficienten* der Formen übertragen, so ist

„das Modulsystem $(M_1, M_2, \dots M_\mu)$ ein das Modulsystem $(M_1', M_2', \dots M_\nu')$ enthaltendes“,

wenn die μ Congruenzen:

$$M_k \equiv 0 \pmod{M_1', M_2', \dots M_\nu'} \qquad (k=1, 2, \dots \mu)$$

bestehen. Das *gegenseitige* Enthalten zweier Modulsysteme begründet hiernach deren Aequivalenz.

Die Gesammtheit der Grössen:

$$A + \sum_{k=1}^{k=\mu} K_k M_k,$$

d. h. derjenigen Grössen, welche man erhält, indem man für K_1, K_2, $\dots K_\mu$ irgend welche ganze ganzzahlige Functionen von $\mathfrak{R}'$, $\mathfrak{R}''$, $\dots \mathfrak{R}^{(n-1)}$ setzt, ist — ähnlich wie oben die specielle Reihe der Zahlen $a + km$ — durch ein System von Invarianten (in endlicher Anzahl) zu charakterisiren, z. B. durch das System eben der Grössen A, M_1, M_2, $\dots M_\mu$, welche hier zur Definition der Gesammtheit von Grössen $A + K_1 M_1 + K_2 M_2 + \cdots + K_\mu M_\mu$ dienen. Ein solches charakteristisches System von Invarianten kann jedoch in mannigfaltiger Weise aufgestellt werden. Die *Anzahl* der zur Charakterisirung sämmtlicher Grössen $A + K_1 M_1 + K_2 M_2 + \cdots + K_\mu M_\mu$ ausreichenden Invarianten bestimmt sich durch die Anzahl der Elemente des Rationalitätsbereichs, also durch die oben mit $n-1$ bezeichnete Zahl. Es kann nämlich erstens als eine der Invarianten irgend eine der Grössen $A + K_1 M_1 + K_2 M_2 + \cdots + K_\mu M_\mu$ selbst gewählt werden. Wird dann zweitens eben diese Grösse von jeder der

anderen subtrahirt, so erhält man die Gesammtheit aller derjenigen Grössen des Rationalitätsbereichs $(\Re', \Re'', \Re''', \ldots \Re^{(n-1)})$, welche das Modulsystem $(M_1, M_2, \ldots M_\mu)$ enthalten, und wenn man alle diese Grössen, unter denen ja auch $M_1, M_2, \ldots M_\mu$ selbst vorkommen, wieder als Elemente eines Modulsystems auffasst, so ist dasselbe dem Modulsysteme $(M_1, M_2, \ldots M_\mu)$ äquivalent. Um also dieses aus jenem zu ermitteln, bedarf es nur eines Verfahrens, mittels dessen die Anzahl der Elemente eines Modulsystems auf eine von vorn herein zu bestimmende Zahl reducirt werden kann, und ein solches Verfahren ergiebt sich, wie ich im § 21 (S. 78[1]) meiner Festschrift zu Herrn *Kummer*'s Doctorjubiläum gezeigt habe, aus der allgemeinen Theorie der Elimination. Durch *diese* sind daher *die Invarianten der Gesammtheit aller unter einander nach irgend einem Modulsystem congruenten ganzen Grössen* des Bereichs $(\Re', \Re'', \ldots \Re^{(n-1)})$ zu ermitteln, indem sie es ermöglicht, ein Modulsystem von beliebig vielen Elementen auf eines zu reduciren, in welchem die Anzahl der Elemente von vorn herein durch die Anzahl der Elemente des Rationalitätsbereichs bestimmt ist.

Die Gesammtheit der (unendlich vielen) Grössen

$$K_1 M_1 + K_2 M_2 + \cdots + K_\mu M_\mu$$

bildet eine besondere Gruppe von Grössen des Rationalitätsbereichs $(\Re', \Re'', \ldots \Re^{(n-1)})$, welche der Kürze halber mit G bezeichnet werden mögen. Ist diese Gruppe auf irgend eine Weise definirt, so kann daraus nach vorstehender Auseinandersetzung das System $(M_1, M_2, \ldots M_\mu)$ oder ein äquivalentes ermittelt werden, d. h. es kann ein System von Grössen, die zur Definition der Gruppe ausreichen, durch arithmetisch-algebraische Methoden aus den definirten Grössen selbst hergeleitet werden. Doch bedarf dies, ebenso wie die dabei benutzte Bildung von Modulsystemen mit unendlich (oder unbestimmt) vielen Elementen einer näheren Präcisirung.

Wird nämlich ein bestimmtes arithmetisch-algebraisches Verfahren vorausgesetzt, mittels dessen alle diejenigen Grössen G_N der zu definirenden Gruppe ganzer ganzzahliger Functionen von $\Re', \Re'', \ldots \Re^{(n-1)}$ aufgestellt werden können, für welche sowohl die Coefficienten als auch die Exponenten

[1]) Bd. II S. 336 flgde. dieser Ausgabe. H.

der verschiedenen Potenzen der Variabeln $\Re$ ihrem absoluten Werthe nach kleiner sind als eine beliebig gegebene Zahl N, und wird ferner eine Bestimmung darüber vorausgesetzt, wie gross N angenommen werden müsse, damit die gesammte Gruppe schon durch die Grössen G_N repräsentirt werde, d. h. damit alle Grössen der Gruppe das aus den Grössen G_N allein gebildete Modulsystem enthalten, so kann bei der obigen Deduction anstatt der aus unendlich (oder unbestimmt) vielen Grössen bestehenden Gesammtheit der ein Modulsystem enthaltenden Grössen von vornherein eine endliche Anzahl derselben zu Grunde gelegt und daher an Stelle jenes dort benutzten Modulsystems mit unendlich vielen Elementen dasjenige gebraucht werden, welches nur die Grössen G_N als Elemente enthält. Die dort erörterte Frage reducirt sich alsdann offenbar nur auf *die*, ein gegebenes beliebig viele Elemente (in endlicher Anzahl) enthaltendes Modulsystem in ein äquivalentes zu transformiren, bei welchem die Anzahl der Elemente eine feste, durch den Rationalitätsbereich $(\Re', \Re'', \ldots \Re^{(n-1)})$ allein bestimmte Zahl nicht überschreitet.

Ohne die hier näher erörterten Voraussetzungen, d. h. also ohne die Möglichkeit, von vorn herein Modulsysteme mit unendlich vielen Elementen durch solche mit einer endlichen Anzahl von Elementen ersetzen zu können, ist aber die Begriffsbildung eines „Modulsystems mit unendlich vielen Elementen" nicht anwendbar. Will man sie dennoch, als eine rein logische, zulassen, so darf dies doch nur unter dem Vorbehalte geschehen, dass bei den speciellen arithmetischen Anwendungen des arithmetisch nicht hinreichend präcisirten Begriffs in jedem einzelnen Falle der Nachweis der Erfüllung jener Voraussetzungen erbracht, d. h. also eigentlich, dass in dem einzelnen Falle die Einführung von Modulsystemen mit unendlich vielen Elementen als unnöthig erwiesen wird.

Nimmt man zu den gewöhnlichen „rationalen" Operationen, nämlich zur Addition, Subtraction, Multiplication und Division, noch die Differentiation hinzu, so genügen freilich Modulsysteme mit einer festen, nur durch die Anzahl der Variabeln bestimmten Anzahl von Elementen nicht mehr, sondern man braucht dann auch Modulsysteme mit einer „unbestimmten" Anzahl von Elementen, d. h. mit einer solchen, die beliebig zu vergrössern ist, und die

also in dem gewöhnlichen Sinne als „unendlich“ bezeichnet werden kann. Aber grade weil die Einführung solcher Modulsysteme erst beim Ueberschreiten der Grenzen der eigentlichen Algebra geboten erscheint, muss sie in den arithmetisch-algebraischen Theorieen vermieden werden*).

Für die Modulsysteme, deren Elemente einem natürlichen Rationalitätsbereiche $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$ angehören, ist der Begriff der „Stufe“ oder des „Ranges“, den ich in meiner Festschrift zu Herrn *Kummer*'s Doctorjubiläum[1]) näher entwickelt habe, von principieller Wichtigkeit. Es giebt, wie a. a. O. im § 21, VII. hervorgehoben ist**), unter den Modulsystemen eines natürlichen Rationalitätsbereichs von $n-1$ unbestimmten Variabeln „reine Modulsysteme erster, zweiter, ... n^{ter} Stufe“ und dem entsprechend auch „reine Formen der n verschiedenen Stufen“.

Ein reines Modulsystem m^{ter} Stufe $(M_1, M_2, \ldots M_\mu)$ kann so beschaffen sein, dass mittels der μ Gleichungen:

$$M_1 = 0, \quad M_2 = 0, \ldots M_\mu = 0$$

eine genau $(n-m-1)$-fache Mannigfaltigkeit aus der $(n-1)$-fachen Mannigfaltigkeit $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$ ausgeschieden wird; es kann aber auch so beschaffen sein, dass ein äquivalentes System $(M_1', M_2', \ldots M_\nu')$ gebildet werden kann, in welchem eines der Elemente z. B. M_ν' eine ganze Zahl ist, während die $\nu - 1$ Gleichungen:

$$M_1' = 0, \quad M_2' = 0, \ldots M_{\nu-1}' = 0$$

eine genau $(n-m)$-fache Mannigfaltigkeit repräsentiren.

Eine „reine Form m^{ter} Stufe“ ist eine solche, in welcher die Coefficienten der Unbestimmten ein reines Modulsystem m^{ter} Stufe bilden; eine solche Form kann aber auch gemäss § 22, IX°. und X°. meiner oben citirten Festschrift dadurch charakterisirt werden, dass sie, nach Multiplication mit einer primitiven Form des Bereichs $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$, sich als lineare homogene Function (mit ganzen, dem Bereich $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$ angehörigen Coefficienten) von genau m Formen darstellen lässt, die mit der darzustellenden Form in ihren Coefficienten völlig übereinstimmen, sich aber durch die Unbestimmten von ihr sowie von einander unterscheiden.

Eine fernere wichtige Eigenschaft der Modulsysteme und der Formen ist ihre Zusammensetzbarkeit im Sinne der Aequivalenz. Die Composition der Formen:

$$M_1X_1 + M_2X_2 + \cdots + M_\mu X_\mu, \quad M_1'X_1' + M_2'X_2' + \cdots + M_\nu'X_\nu'$$

erfolgt durch wirkliche Multiplication, die der Modulsysteme also durch die Bildung eines neuen, dessen Elemente die $\mu\nu$ Producte:

$$M_h M_k' \qquad \begin{pmatrix} h = 1, 2, \ldots \mu \\ k = 1, 2, \ldots \nu \end{pmatrix}$$

sind. Hieran knüpft sich unmittelbar die Frage der Möglichkeit der Decomposition eines gegebenen Modulsystems oder einer gegebenen Form. Wie es nun offenbar Modulsysteme und Formen giebt, die solchen äquivalent sind, welche durch Composition aus anderen gebildet werden können, so giebt es auch Modulsysteme und Formen, bei denen dies nicht der Fall ist, und die deshalb als „nicht zerlegbar (im Sinne der Aequivalenz)“ zu bezeichnen

*) Die obigen Erwägungen stehen, wie mir scheint, der Einführung jener *Dedekind*'schen Begriffsbildungen wie „Modul“, „Ideal“ u. s. w. entgegen; ebenso auch der Einführung der verschiedenen Begriffsbildungen, mit Hülfe deren in neuerer Zeit vielfach (zuerst wohl von *Heine*) versucht worden ist, das „Irrationale“ ganz allgemein zu fassen und zu begründen. Selbst der *allgemeine* Begriff einer unendlichen Reihe, z. B. einer solchen, die nach bestimmten Potenzen von Variabeln fortschreitet, ist meines Erachtens nur mit dem Vorbehalte zulässig, dass in jedem speciellen Falle auf Grund des arithmetischen Bildungsgesetzes der Glieder (oder der Coefficienten), ähnlich wie oben, gewisse Voraussetzungen als erfüllt nachgewiesen werden, welche die Reihen wie endliche Ausdrücke anzuwenden gestatten, und welche also das Hinausgehen über den Begriff einer *endlichen* Reihe eigentlich unnöthig machen.

**) Vgl. auch die ausführlicheren Auseinandersetzungen in Herrn *Molk*'s Abhandlung: „Sur une notion qui comprend celle de la divisibilité et sur la théorie générale de l'élimination“ Chapitre III. Acta Mathematica Tome VI.

[1]) Band II S. 237—387 dieser Ausgabe. Vgl. S. 336. H.

sind. Aber unter den nicht zerlegbaren Modulsystemen oder Formen giebt es doch noch solche, die andere Modulsysteme oder Formen derselben Stufe „enthalten“, wie ich am Schlusse des § 21 meiner mehrerwähnten Festschrift hervorgehoben habe, und es empfiehlt sich desshalb, unter den nicht zerlegbaren Modulsystemen und Formen noch diejenigen in besonderer Weise zu kennzeichnen, bei denen dies nicht der Fall ist, welche also keine anderen Modulsysteme oder Formen derselben Stufe unter sich enthalten. Für diese *besonderen* nicht zerlegbaren Modulsysteme und Formen soll nunmehr die Bezeichnung als:

„Primmodulsysteme“ und „Primformen“

vorbehalten werden, welche ich in den §§ 21, VI und 22, VI meiner Festschrift als völlig gleichbedeutend mit der Bezeichnung der Systeme und Formen als „nicht zerlegbare“ angewandt habe.

Es werden hauptsächlich *Primmodulsysteme* eines natürlichen Rationalitätsbereichs $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$ von einem bestimmten m^{ten} Range, in dem eben dargelegten engeren Sinne, im Folgenden zur Anwendung kommen. Für solche Modulsysteme theilen sich die sämmtlichen ganzen Grössen des Rationalitätsbereichs $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$ in zwei Gruppen, von denen die eine alle das Modulsystem enthaltenden Grössen, die andere alle übrigen umfasst. Die Grössen dieser anderen, durch ein Primmodulsystem m^{ter} Stufe aus dessen Integritätsbereich $[\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)}]$ ausgesonderten Gruppe können ihrerseits so charakterisirt werden, dass sie mit dem Primmodulsystem zusammen Modulsysteme $(m+1)^{ter}$ Stufe bilden, oder dass sie (nach dem Primmodulsysteme) Formen $(m+1)^{ter}$ Stufe congruent sind, d. h. also solchen Formen, die für Modulsysteme m^{ter} Stufe (uneigentlich) primitive oder Einheits-Formen sind*).

Denn, wenn $(M_1, M_2, \ldots M_\mu)$ ein Primmodulsystem m^{ter} Stufe und M_0 irgend eine Grösse des Integritätsbereichs $[\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)}]$ bedeutet, so ist

*) Vgl. § 22, VII der mehrfach citirten Festschrift[1]).

[1]) Bd. II S. 344 dieser Ausgabe. H.

das Modulsystem $(M_0, M_1, M_2, \ldots M_\mu)$ offenbar in $(M_1, M_2, \ldots M_\mu)$ enthalten, und da dieses, als Primmodulsystem, keine *anderen* Modulsysteme m^{ter} Stufe enthält, so muss das Modulsystem $(M_0, M_1, M_2, \ldots M_\mu)$ entweder mit $(M_1, M_2, \ldots M_\mu)$ äquivalent oder aber ein System $(m+1)^{ter}$ Stufe sein. Im ersteren Falle muss M_0 nach dem Modulsysteme $(M_1, M_2, \ldots M_\mu)$ congruent Null und also eine Grösse der *ersten* von jenen zwei Gruppen sein. Es muss daher, wenn M_0 der *zweiten* Gruppe angehört, $(M_0, M_1, M_2, \ldots M_\mu)$ ein Modulsystem $(m+1)^{ter}$ Stufe und $M_0 + U_1 M_1 + \cdots + U_\mu M_\mu$ eine Form $(m+1)^{ter}$ Stufe sein, welcher M_0 selbst offenbar nach dem Modulsystem $(M_1, M_2, \ldots M_\mu)$ congruent ist. Jede Grösse des Integritätsbereichs $[\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)}]$ ist also *modulis* $M_1, M_2, \ldots M_\mu$, wenn dies ein *Prim*modulsystem ist, entweder der Null oder einer Einheitsform congruent.

So ist z. B. für das Primmodulsystem zweiter Stufe $(\mathfrak{R}', \mathfrak{R}'')$ die Variable $\mathfrak{R}'''$ eine Grösse der zweiten Gruppe und der Form:

$$\mathfrak{R}' X + \mathfrak{R}'' Y + \mathfrak{R}'''$$

congruent, welche an sich eine Form dritter Stufe, aber für Modulsysteme zweiter Stufe als eine uneigentlich primitive oder Einheits-Form zu bezeichnen ist. Es bildet ferner die Grösse $\mathfrak{R}'''$ mit dem Modulsystem $(\mathfrak{R}', \mathfrak{R}'')$ zusammen das Modulsystem $(\mathfrak{R}', \mathfrak{R}'', \mathfrak{R}''')$, welches offenbar den Rang *drei* hat. So ist ferner für eine gewöhnliche Primzahl p die Gesammtheit der ganzen Zahlen in zwei Gruppen zu theilen, deren eine die sämmtlichen durch p theilbaren Zahlen umfasst, während jede der übrigen Zahlen *modulo* p offenbar unter der Zahl *Eins* enthalten, also eine *Einheit* ist. Denn für jede durch p nicht theilbare Zahl r existirt ja eine Zahl s, welche der Congruenz: $rs \equiv 1 \pmod{p}$ genügt. Jede ganze Zahl ist also *modulo* p entweder *Null* oder *Einheit*.

Wenn das Product von zwei ganzen Grössen des Rationalitätsbereichs $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$ eine Grösse der ersten von den beiden Gruppen ist, in welche sich die sämmtlichen ganzen Grössen des Bereichs für ein Primmodulsystem theilen, so muss mindestens eine der beiden Grössen selbst der ersten Gruppe angehören, d. h.

der Fundamentalsatz der gewöhnlichen Zahlentheorie, dass ein Product nur dann für einen Primzahlmodul congruent Null sein kann, wenn einer der Factoren congruent Null ist, gilt auch für allgemeine *Primmodulsysteme.*

Denn wenn $M_1, M_2, \ldots M_\mu$ die Elemente eines Primmodulsystems und M, M_0 irgend zwei Grössen des Integritätsbereichs $[\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)}]$ bedeuten, so folgt aus der Congruenz:

$$MM_0 \equiv 0 \pmod{M_1, M_2, \ldots M_\mu},$$

dass auch das Product der beiden Formen:

$$M + U_1M_1 + U_2M_2 + \cdots + U_\mu M_\mu, \quad M_0 + U_1M_1 + U_2M_2 + \cdots + U_\mu M_\mu$$

das Primmodulsystem $(M_1, M_2, \ldots M_\mu)$ enthalten muss. *Beide* Formen können also nicht für dieses Primmodulsystem eigentlich oder uneigentlich primitiv sein. Dies würde aber der Fall sein, wenn beide Grössen M, M_0 zur Gruppe derjenigen gehörten, die das Modulsystem nicht enthalten.

Auf den Gedanken, den *Gauss*'schen Begriff der Congruenz für Zahlenmoduln zu einem Begriffe der Congruenz für beliebige Modulsysteme zu erweitern, bin ich vor etwa 30 Jahren durch gleichzeitige Beschäftigung mit algebraischen und arithmetischen Untersuchungen geführt worden, und ich habe diesen Gedanken schon im Jahre 1858 vielen Mathematikern (vor Allen *Dirichlet*, *Kummer*, *Weierstrass*) in mündlicher Unterhaltung, seit dem Jahre 1862 aber auch in meinen Universitätsvorlesungen mitgetheilt und dadurch in weiteren Kreisen verbreitet. Durch den Druck habe ich die Elemente der Theorie der Modulsysteme erst in meiner Festschrift zu Herrn *Kummer*'s Doctorjubiläum veröffentlicht und dort hauptsächlich Anwendungen auf rein arithmetische Fragen beigefügt. Dass aber die Theorie der Modulsysteme auch bei ganz elementaren *algebraischen* Fragen mit Erfolg anzuwenden ist, indem sie die Methoden durchsichtiger erscheinen, die Resultate zugleich präciser und allgemeiner fassen lässt, soll hier an einigen, auch an sich interessanten Beispielen dargelegt werden.

II.

Lineare Congruenzen für Primmodulsysteme.

Bildet man aus $t \cdot t'$, in t Zeilen von je t' Elementen geordneten, unbestimmten Variabeln die Determinanten irgend einer (r^{ten}) Ordnung und bezeichnet dieselben (in beliebiger Reihenfolge) mit:

$$V_1^{(r)}, \quad V_2^{(r)}, \quad V_3^{(r)}, \ldots,$$

so kann man die $t \cdot t'$ unbestimmten Variabeln selbst, von denen man ausgegangen ist, als Determinanten erster Ordnung, analog mit:

$$V_{ik}^{(1)} \qquad \binom{i=1, 2, \ldots t}{k=1, 2, \ldots t'}$$

bezeichnen. Nimmt man nun noch t' unbestimmte Variable:

$$X_1, \quad X_2, \ldots X_{t'}$$

hinzu und setzt:

$$(1.) \qquad V_{i0}^{(1)} = \sum_k V_{ik}^{(1)} X_k \qquad \binom{i=1, 2, \ldots t}{k=1, 2, \ldots t'},$$

so ist die Determinante:

$$\left| V_{gh}^{(1)} \right| \qquad \binom{g=1, 2, \ldots r, s}{h=0, 1, \ldots r}$$

eine lineare homogene Function der t' Variabeln X, deren Coefficienten sämmtlich Determinanten $(r+1)^{\text{ter}}$ Ordnung des Systems:

$$V_{ik}^{(1)} \qquad \binom{i=1, 2, \ldots t}{k=1, 2, \ldots t'}$$

sind. Auf Grund der Theorie der Modulsysteme wird dies vollständig durch die Congruenz:

$$(2.) \qquad \left| V_{gh}^{(1)} \right| \equiv 0 \pmod{V_1^{(r+1)}, V_2^{(r+1)}, V_3^{(r+1)}, \ldots} \qquad \binom{g=1, 2, \ldots r, s}{h=0, 1, 2, \ldots r}$$

ausgedrückt, in welcher als Elemente des Modulsystems die *sämmtlichen* Determinanten $(r+1)^{ter}$ Ordnung des Variablen-Systems:

$$V_{ik}^{(1)} \qquad \binom{i=1,2,\dots t}{k=1,2,\dots t'}$$

zu nehmen sind.

Entwickelt man nun die Determinante in der Congruenz (2.) nach den Elementen $V_{g0}^{(1)}$, so resultirt die Congruenz:

$$(3.) \qquad V_{11}^{(r)} V_{s0}^{(1)} \equiv 0 \pmod{V_{10}^{(1)}, V_{20}^{(1)}, \dots V_{r0}^{(1)}; V_1^{(r+1)}, V_2^{(r+1)}, \dots},$$

in welcher $V_{11}^{(r)}$ die Determinante:

$$|V_{ik}^{(1)}| \qquad (i,k=1,2,\dots r)$$

bedeutet, und welche offenbar nicht bloss für $s>r$, sondern auch für $s \leqq r$, also für alle t Werthe $s=1, 2, \dots t$ besteht.

Setzt man ferner, wenn l eine der Zahlen $1, 2, \dots r$ und m eine der Zahlen $0, 1, 2, \dots t$ bedeutet:

$$V_{im}^{(r)} = |V_{ik}^{(1)}| \qquad \left(\begin{smallmatrix} i=1,2,\dots r \\ k=1,2,\dots l-1,\ m,\ l+1,\dots r \end{smallmatrix}\right),$$

so wird für diejenigen Werthe von m, die nicht grösser als r sind:

$$V_{im}^{(r)} = \delta_{lm} V_{11}^{(r)} \qquad (l,m=1,2,\dots r),$$

wenn $\delta_{lm}=0$ oder $\delta_{lm}=1$ ist, je nachdem $l \gtrless m$ oder $l=m$ ist, und für $m=0$ wird:

$$(4.) \qquad V_{i0}^{(r)} = \sum_n |V_{ik}^{(r)}| X_n \qquad \left(\begin{smallmatrix} i=1,2,\dots r;\ 1 \leqq i \leqq r \\ k=1,2,\dots l-1,\ n,\ l+1,\dots r \\ n=l,\ r+1,\ r+2,\dots t \end{smallmatrix}\right).$$

Die Determinante $V_{i0}^{(r)}$ wird also eine lineare homogene Function von:

$$X_i,\ X_{r+1},\ X_{r+2},\ \dots\ X_{t'},$$

deren Coefficienten selbst Determinanten r^{ter} Ordnung sind; und zwar ist der Coefficient von X_i für jeden Werth von l eine und dieselbe Determinante r^{ter} Ordnung:

$$|V_{ik}^{(1)}| \qquad (i,k=1,2,\dots r),$$

welche schon oben mit $V_{11}^{(r)}$ bezeichnet worden ist.

Andererseits ist aber $V_{i0}^{(r)}$ offenbar eine lineare homogene Function der r Grössen $V_{10}^{(1)}, V_{20}^{(1)}, \dots V_{r0}^{(1)}$; und es besteht daher die Congruenz:

$$V_{i0}^{(r)} \equiv 0 \pmod{V_{10}^{(1)}, V_{20}^{(1)}, \dots V_{r0}^{(1)}} \qquad (i=1,2,\dots r),$$

in welcher, der Natur der Sache nach, dem Modulsysteme rechts noch beliebige Elemente hinzugefügt werden können. So ist also auch:

$$(5.) \qquad V_{i0}^{(r)} \equiv 0 \pmod{V_{10}^{(1)}, V_{20}^{(1)}, \dots V_{i0}^{(1)}}$$

für jeden der r Indices $i=1, 2, \dots r$.

In der Entwickelung der schon oben betrachteten Determinante:

$$|V_{gh}^{(1)}| \qquad \left(\begin{smallmatrix} g=1,2,\dots r,\ s \\ h=0,1,\dots r \end{smallmatrix}\right)$$

nach den Elementen $V_{s0}^{(1)}, V_{s1}^{(1)}, \dots V_{sr}^{(1)}$ ist das erste, nämlich $V_{s0}^{(1)}$ mit $V_{11}^{(r)}$ und aber irgend eines der folgenden Elemente $V_{si}^{(1)}$ mit $V_{i0}^{(r)}$ multiplicirt. Es besteht daher die Congruenz:

$$|V_{gh}^{(1)}| \equiv V_{11}^{(r)} V_{s0}^{(1)} \pmod{V_{10}^{(r)}, V_{20}^{(r)}, \dots V_{r0}^{(r)}},$$

und wenn man s gleich einer der Zahlen $1, 2, \dots r$ setzt, so dass die Determinante links verschwindet, so geht diese Congruenz in folgende über:

$$(6.) \qquad V_{11}^{(r)} V_{i0}^{(1)} \equiv 0 \pmod{V_{10}^{(r)}, V_{20}^{(r)}, \dots V_{r0}^{(r)}} \qquad (i=1,2,\dots r).$$

Wenn man nun in der obigen Congruenz (3.) den Ausdruck auf der linken Seite und auch die ersten r Elemente des Modulsystems mit $V_{11}^{(r)}$ multiplicirt, so erhält man die Congruenz:

$$V_{11}^{(r)} V_{11}^{(r)} V_{i0}^{(1)} \equiv 0 \quad (\text{modd. } V_{11}^{(r)} V_{10}^{(1)},\ V_{11}^{(r)} V_{20}^{(1)},\ \ldots\ V_{11}^{(r)} V_{r0}^{(1)};\ V_1^{(r+1)},\ V_2^{(r+1)},\ \ldots),$$

welche für alle Indices $s = 1, 2, \ldots t$ gültig bleibt, und man kann darin die r ersten Elemente des Modulsystems auf Grund der Congruenz (6.) durch die Elemente $V_{10}^{(r)},\ V_{20}^{(r)},\ \ldots\ V_{r0}^{(r)}$ ersetzen.

Man gelangt hierdurch zu der Congruenz:

(7.) $$V_{11}^{(r)} V_{11}^{(r)} V_{i0}^{(1)} \equiv 0 \quad (\text{modd. } V_{10}^{(r)},\ V_{20}^{(r)},\ \ldots\ V_{r0}^{(r)};\ V_1^{(r+1)},\ V_2^{(r+1)},\ \ldots),$$

welche in Verbindung mit der Congruenz (5.) das Ziel der vorstehenden Entwickelungen bildet. Die beiden Congruenzen (5.) und (7.) zeigen,

> dass einerseits das Modulsystem $(V_{10}^{(1)},\ V_{20}^{(1)},\ \ldots\ V_{t0}^{(1)})$ in dem Modulsysteme $(V_{10}^{(r)},\ V_{20}^{(r)},\ \ldots\ V_{r0}^{(r)})$ enthalten ist, und dass andererseits dieses letztere Modulsystem unter Hinzunahme der Elemente $V_1^{(r+1)},\ V_2^{(r+1)},\ \ldots$ in dem ersteren enthalten ist, wenn dessen Elemente sämmtlich mit dem Quadrate der Determinante $V_{11}^{(r)}$ multiplicirt werden.

Dieses Resultat lässt sich auch folgendermassen formuliren:

> Im Sinne einer Congruenz für das aus allen Determinanten $(r+1)^{\text{ter}}$ Ordnung $V_1^{(r+1)},\ V_2^{(r+1)},\ \ldots$ gebildete Modulsystem lässt sich einerseits jeder der r Ausdrücke $V_{i0}^{(r)}$ für $i = 1, 2, \ldots r$, d. i.
>
> $$V_{11}^{(r)} X_i + \sum_{n=r+1}^{n=t'} \left| V_{hk}^{(r)} \right| X_n \qquad \left(\begin{smallmatrix} h=1,\ 2,\ \ldots\ r \\ k=1,\ 2,\ \ldots\ i-1,\ n,\ i+1,\ \ldots\ r \end{smallmatrix}\right),$$

> als ganze lineare homogene Function der t mit $V_{10}^{(1)},\ V_{20}^{(1)},\ \ldots\ V_{t0}^{(1)}$ bezeichneten Ausdrücke:
>
> $$\sum_{k=1}^{k=t'} V_{ik}^{(1)} X_k \qquad (i = 1, 2, \ldots t),$$
>
> andererseits aber auch jeder dieser letzteren t Ausdrücke, nach Multiplication mit dem Quadrate der Determinante r^{ter} Ordnung $V_{11}^{(r)}$, als ganze lineare homogene Function der ersteren r Ausdrücke $V_{i0}^{(r)}$ darstellen, und zwar so, dass die sämmtlichen Coefficienten ganze ganzzahlige Functionen der $t'(t+1)$ unbestimmten Variabeln:
>
> $$V_{ik}^{(1)},\quad X_k \qquad \left(\begin{smallmatrix} i=1,\ 2,\ \ldots\ t \\ k=1,\ 2,\ \ldots\ t' \end{smallmatrix}\right)$$
>
> sind.

Werden an Stelle der tt' unbestimmten Variabeln $V_{ik}^{(1)}$ irgend welche ganze Grössen eines natürlichen Rationalitätsbereichs $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$ genommen, für welche die sämmtlichen Determinanten $(r+1)^{\text{ter}}$ Ordnung ein bestimmtes Primmodulsystem $(M, M', M'', \ldots)$ des Rationalitätsbereichs $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$ enthalten, während die Determinante $V_{11}^{(r)}$ eben dieses Primmodulsystem *nicht* enthält, so lässt sich aus dem eben formulirten Resultat unmittelbar erschliessen, dass die beiden Systeme von linearen Congruenzen:

(8.) $$\sum_{k=1}^{k=t'} V_{ik}^{(1)} X_k \equiv 0 \quad (\text{modd. } M,\ M',\ M'',\ \ldots) \qquad (i = 1, 2, \ldots t),$$

(9.) $$V_{11}^{(r)} X_i + \sum_{n=r+1}^{n=t'} \left| V_{hk}^{(r)} \right| X_n \equiv 0 \quad (\text{modd. } M,\ M',\ M'',\ \ldots)$$

$$\left(\begin{smallmatrix} h,\ i=1,\ 2,\ \ldots\ r \\ k=1,\ 2,\ \ldots\ i-1,\ n,\ i+1,\ \ldots\ r \end{smallmatrix}\right)$$

mit einander völlig äquivalent sind, d. h. also dass beide genau dieselben Bestimmungen für die zu bestimmenden t' Grössen X enthalten.

Nach den in früheren Aufsätzen eingeführten Bezeichnungen*) ist r die „*Rang-* oder *Stufenzahl*“ des Systems $V_{ik}^{(1)}$ „*in Beziehung auf das Primmodulsystem* $(M, M', M'', \ldots)$“, weil jede der Determinanten $(r+1)^{\text{ter}}$ Ordnung, nicht aber jede der Determinanten r^{ter} Ordnung (modd. $M, M', M'', \ldots$) congruent Null ist. Betrachtet man die Grössen $V_{ik}^{(1)}$ als die gegebenen, die Grössen X_k aber als die gesuchten, gemäss den Congruenzen (8.) zu bestimmenden, so sind es die Congruenzen (9.), welche die vollständige Auflösung der ersteren enthalten. Da nun in den Congruenzen (9.) offenbar die $t'-r$ Grössen $X_{r+1}, X_{r+2}, \ldots X_{t'}$ unbestimmt gelassen werden können und nur die r Grössen $X_1, X_2, \ldots X_r$ sich als lineare homogene Functionen jener $t'-r$ übrigen bestimmen, so zeigt sich, dass

durch ein System von Congruenzen:

$$\sum_{k=1}^{k=t'} V_{ik}^{(1)} X_k \equiv 0 \quad (\text{modd. } M,\ M',\ M'', \ldots) \qquad (i=1, 2, \ldots t),$$

in welchem $V_{ik}^{(1)}$, M, M', M'', ... beliebige Grössen eines natürlichen Rationalitätsbereichs bedeuten und die letzteren ein *Primmodulsystem* bilden, die t'-fache Mannigfaltigkeit der Grössen X auf eine genau $(t'-r)$-fache Mannigfaltigkeit eingeschränkt wird, wenn die Zahl r den Rang des Systems $V_{ik}^{(1)}$ in Beziehung auf das Modulsystem $(M, M', M'', \ldots)$ bezeichnet.

Es verdient hervorgehoben zu werden, dass dieses ganz allgemeine Resultat auf die zugleich einfachste und vollständigste Weise durch die beiden obigen Congruenzen (5.) und (7.) dargestellt wird, und zwar wird es dort, da die Congruenzen für Modulsysteme, ihrer Definition nach, das Bestehen gewisser Gleichungen ausdrücken,

*) Vgl. Art. X meines Aufsatzes: „Die Periodensysteme von Functionen reeller Variabeln“ im Sitzungsbericht der hiesigen Akademie vom 20. Nov. 1884, Stück XLVI S. 1078[1]).

[1]) Band III S. 43 dieser Ausgabe von *L. Kronecker's* Werken. H.

in der Form identischer Gleichungen präciser, übersichtlicher und allgemeiner gefasst,

als es jemals bisher geschehen ist. Das Streben, den mathematischen Resultaten eine solche, meines Erachtens nicht nur wünschenswerthe, sondern eigentlich allein in Beziehung auf Klarheit und Sicherheit befriedigende Fassung zu geben, hat mich bei der Einführung der Divisoren-Systeme so wie bei den vorliegenden Anwendungen derselben geleitet. Dass bei complicirteren Fragen die Bemühungen, sie in der hier charakterisirten vollendeten Weise zu lösen, vorläufig noch schwierig oder gar aussichtslos erscheinen, darf von der Fortsetzung solcher Bemühungen nicht abhalten.

Für den speciellen Fall des absoluten Rationalitätsbereichs $\mathfrak{R}=1$ sind die Elemente $V_{ik}^{(1)}$ gewöhnliche ganze Zahlen und an Stelle des Primmodulsystems $(M, M', M'', \ldots)$ tritt ein gewöhnlicher Primzahl-Modul p. Die t' Congruenzen:

$$\sum_{k=1}^{k=t'} V_{ik}^{(1)} X_k \equiv 0 \pmod{p} \qquad (i=1, 2, \ldots t) \tag{8}$$

werden also durch eine genau $(t'-r)$-fache Mannigfaltigkeit von Werthen X befriedigt, wenn das System der tt' Zahlen $V_{ik}^{(1)}$ in Beziehung auf den Modul p vom Range r ist*).

Man kann die Rangzahl r hier, indem man die t' Grössen X als unbestimmte Variable betrachtet, auch dadurch charakterisiren, dass $r+1$ die Stufenzahl des Divisorensystems:

$$(p,\ \sum_k V_{1k}^{(1)} X_k,\ \sum_k V_{2k}^{(1)} X_k, \ldots \sum_k V_{tk}^{(1)} X_k) \qquad (k=1, 2, \ldots t')$$

angiebt, dessen $t+1$ Elemente dem Rationalitätsbereich $(X_1, X_2, \ldots X_{t'})$ angehören.

*) Hierin liegt eine ausdrückliche Rechtfertigung jenes Ausspruches von Hrn. *Rados* auf S. 259 dieses Bandes[1]), womit der erste Absatz schliesst: „Ganz ebenso aber u. s. w.“

[1]) *Gustav Rados*, Zur Theorie der Congruenzen höheren Grades, Crelle's Journal für Mathematik. Bd. 99 S. 258—260. H.

Werden die tt' Grössen $V_{ik}^{(1)}$, wie im Anfange dieses Artikels, als unbestimmte Variable aufgefasst, so ist das aus allen Subdeterminanten $(r+1)^{\text{ter}}$ Ordnung gebildete Divisorensystem:

$$(V_1^{(r+1)},\quad V_2^{(r+1)},\ldots)$$

ein System von der Stufenzahl $(t-r)(t'-r)$, jedoch ein solches, dem Systeme höherer Stufen beigemischt sind. Denn erstens enthält jede der $(t-r)(t'-r)$ Determinanten $(r+1)^{\text{ter}}$ Ordnung:

$$|V_{gh}^{(1)}| \qquad \binom{g=1,2,\ldots r,i}{h=1,2,\ldots r,k},$$

welche den Indexwerthen:

$$i=r+1,\ r+2,\ldots t;\qquad k=r+1,\ r+2,\ldots t'$$

entsprechen, ein Element, nämlich $V_{ik}^{(1)}$, welches in den übrigen nicht vorkommt. Das aus diesen Determinanten gebildete Divisorensystem:

(10.) $$(V_1^{(r+1)},\ V_2^{(r+1)},\ \ldots\ V_\varrho^{(r+1)}),$$

in welchem zur Abkürzung:

$$(t-r)(t'-r)=\varrho$$

gesetzt ist, hat also die Stufenzahl ϱ.

Entwickelt man nun zweitens eine dieser ϱ Determinanten nach den Elementen der letzten Horizontalreihe, so kommt:

$$V_{ik}^{(1)}V_{kk}^{(r)}+\sum_{m=1}^{m=r}V_{im}^{(1)}V_{mk}^{(r)}=|V_{gh}^{(1)}| \qquad \binom{g=1,2,\ldots r,i}{h=1,2,\ldots r,k},$$

und es ist hierbei $V_{kk}^{(r)}=V_{11}^{(r)}$. Da die Determinante rechts für $i>r$, $k>r$

eben eines der Elemente jenes Divisorensystems (10.), für alle anderen Werthe von i und k aber gleich Null ist, so besteht die Congruenz:

$$V_{11}^{(r)}V_{ik}^{(1)}\equiv-\sum_{m=1}^{m=r}V_{im}^{(1)}V_{mk}^{(r)}\quad(\text{modd. } V_1^{(r+1)},\ V_2^{(r+1)},\ \ldots\ V_\varrho^{(r+1)})$$

offenbar für *alle* Werthe von i und k, d. h. für $i=1,2,\ldots t$ und $k=1,2,\ldots t'$. Jedes System von $(r+1)^2$ Grössen:

$$\sum_{m=1}^{m=r}V_{im}^{(1)}V_{mk}^{(r)} \qquad \binom{i=i_0,\ i_1,\ldots i_r}{k=k_0,\ k_1,\ldots k_r}$$

ist aber offenbar aus den beiden Systemen von je $r(r+1)$ Elementen:

$$V_{im}^{(1)},\qquad V_{mk}^{(r)} \qquad \binom{i=i_0,\ i_1,\ldots i_r}{k=k_0,\ k_1,\ldots k_r}{m=1,\ 2,\ \ldots\ r}$$

zusammengesetzt; die aus je $(r+1)^2$ Grössen:

$$V_{11}^{(r)}V_{ik}^{(1)} \qquad \binom{i=i_0,\ i_1,\ldots i_r}{k=k_0,\ k_1,\ldots k_r}$$

gebildete Determinante ist daher für jenes Modulsystem $(V_1^{(r+1)},\ V_2^{(r+1)},\ldots V_\varrho^{(r+1)})$ congruent Null, d. h.

> *jede* der Determinanten $(r+1)^{\text{ter}}$ Ordnung des Systems $V_{ik}^{(1)}$ enthält, nach Multiplication mit $\left(V_{11}^{(r)}\right)^{r+1}$, dasjenige Modulsystem, dessen Elemente jene besonderen ϱ Determinanten $(r+1)^{\text{ter}}$ Ordnung: $V_1^{(r+1)},\ V_2^{(r+1)},\ \ldots\ V_\varrho^{(r+1)}$ sind.

Das aus *allen* Determinanten $(r+1)^{\text{ter}}$ Ordnung zu bildende Modulsystem enthält also ausser dem Modulsystem ϱ^{ter} Stufe:

$$(V_1^{(r+1)},\ V_2^{(r+1)},\ \ldots\ V_\varrho^{(r+1)})$$

noch dasjenige höherer Stufe, welches entsteht, wenn man diesen ϱ Deter-

minanten $(r+1)^{\text{ter}}$ Ordnung die mit $V_{11}^{(r)}$ bezeichnete Determinante r^{ter} Ordnung hinzufügt.

Der Sache nach ist diese letztere Entwickelung bereits im Art. I meiner „Bemerkungen zur Determinanten-Theorie" enthalten*), aber ihre eigentliche Bedeutung konnte erst hier mit Hülfe der Theorie der Modulsysteme dargelegt werden.

III.

Darstellung des grössten gemeinsamen Theilers von zwei ganzen Functionen von x für irgend ein Primmodulsystem des Bereichs ihrer Coefficienten.

§ 1.

Bezeichnet man mit x, $\mathfrak{v}_0$, $\mathfrak{v}_1$, $\dots$ $\mathfrak{v}_{n-1}$, v_0, v_1, $\dots$ v_{n-1} unbestimmte Variable und setzt:

$$\mathfrak{V}(x)=\mathfrak{v}_0+\mathfrak{v}_1x+\mathfrak{v}_2x^2+\cdots+\mathfrak{v}_{n-1}x^{n-1}, \qquad V(x)=v_0+v_1x+v_2x^2+\cdots+v_{n-1}x^{n-1}+x^n,$$

$$\frac{\mathfrak{V}(x)}{V(x)}=w_0x^{-1}+w_1x^{-2}+w_2x^{-3}+\cdots \text{ in inf.},$$

so sind w_0, w_1, w_2, $\dots$ ganze ganzzahlige Functionen der Variabeln $\mathfrak{v}$ und v. Bedeutet nun m irgend eine Zahl, die kleiner als n oder auch gleich n ist, und nimmt man:

$$a_{00}=w, \quad a_{0k}=a_{k0}=-w_{k-1}, \qquad a_{ik}=a_{ki}=w_{i+k-2}x-w_{i+k-1} \qquad (i,\ k=1,\ 2,\ \dots\ m),$$

so werden durch die Gleichung:

$$(\mathfrak{A}.) \qquad |a_{gh}|=w\,V^{(m)}(x)-\mathfrak{V}^{(m)}(x) \qquad (g,\ h=0,\ 1,\ 2,\ \dots\ m)$$

*) Bd. 72 dieses Journals S. 152[1]).

[1]) Band I S. 238—239 dieser Ausgabe von *L. Kronecker*'s Werken. H.

zwei ganze Functionen von x:

$$V^{(m)}(x), \quad \mathfrak{V}^{(m)}(x)$$

definirt, von denen die erstere vom m^{ten}, die letztere vom $(m-1)^{\text{ten}}$ Grade ist. Eben diese beiden Functionen von x können aber auch in folgender Weise definirt werden:

$$(\mathfrak{A}'.) \qquad V^{(m)}(x)=|w_{i+k-2}\,x-w_{i+k-1}|, \quad \mathfrak{V}^{(m)}(x)=\sum_{i,k}w_iw_k\,V_{ik}^{(m)}(x) \qquad (i,\ k=1,\ 2,\ \dots\ m),$$

wenn $V_{ik}^{(m)}(x)$ die „*Adjuncte*" des Elementes $w_{i+k-2}x-w_{i+k-1}$ in der Determinante $V^{(m)}(x)$ bedeutet und also durch die Gleichung:

$$V_{ik}^{(m)}(x)=\frac{\partial|a_{\mathfrak{ik}}|}{\partial a_{ik}} \qquad \binom{\mathfrak{i},\ \mathfrak{k}=1,\ 2,\ \dots\ m}{i,\ k=1,\ 2,\ \dots\ m}$$

erklärt wird. Bezeichnet man endlich noch die Determinante:

$$|w_{i+k}| \qquad (i,\ k=0,\ 1,\ \dots\ m-1),$$

welche den Coefficienten von x^m in $V^{(m)}(x)$ bildet, mit V_m, so ist:

$$\frac{\partial|a_{gh}|}{\partial a_{00}}=V^{(m)}(x), \qquad \frac{\partial^2|a_{gh}|}{\partial a_{00}\partial a_{mm}}=V^{(m-1)}(x),$$

$$\frac{\partial|a_{gh}|}{\partial a_{mm}}=w\,V^{(m-1)}(x)-\mathfrak{V}^{(m-1)}(x), \qquad \binom{g,\ h=0,\ 1,\ \dots\ m}{i,\ k=0,\ 1,\ \dots\ m-1},$$

$$\frac{\partial|a_{gh}|}{\partial a_{0m}}=-\frac{\partial|a_{gh}|}{\partial a_{m0}}=|w_{i+k}|=V_m,$$

und die bekannte Determinantenformel:

$$\frac{\partial|a_{gh}|}{\partial a_{00}}\,\frac{\partial|a_{gh}|}{\partial a_{mm}}-\frac{\partial|a_{gh}|}{\partial a_{0m}}\,\frac{\partial|a_{gh}|}{\partial a_{m0}}=|a_{gh}|\cdot\frac{\partial^2|a_{gh}|}{\partial a_{00}\partial a_{mm}} \qquad (g,\ h=0,\ 1,\ \dots\ m)$$

liefert demnach die Relation:

$$(\mathfrak{B}.) \qquad \mathfrak{V}^{(m)}(x)\,V^{(m-1)}(x) - \mathfrak{V}^{(m-1)}(x)\,V^{(m)}(x) = V_m^2.$$

Für jedes beliebige System von $(m+1)^2$ Grössen a_{gh} besteht offenbar die Determinantengleichung:

$$(\mathfrak{C}.) \qquad \Big|\sum_f a_{gf}x^{h-f}\Big| = |a_{gh}| \qquad \binom{f=0,\,1,\,2,\,\dots\,h}{g,\,h=0,\,1,\,2,\,\dots\,m}.$$

Da nun bei den oben angenommenen Werthen von a_{gh}:

$$\sum_{f=0}^{f=h} a_{0f}x^{h-f} = \Big(w - \sum_{f=1}^{f=h} w_{f-1}x^{-f}\Big)x^h$$

und aber für $g>0$:

$$\sum_{f=0}^{f=h} a_{gf}x^{h-f} = -\,w_{g+h-1}$$

wird, so geht jene Determinanten-Gleichung ($\mathfrak{C}.$) mit Berücksichtigung der Gleichung ($\mathfrak{A}.$) in folgende über:

$$(\mathfrak{D}.) \qquad \Big|w_h,\ w_{h+1},\ \dots\ w_{h+m-1},\ wx^h - \sum_{f=1}^{f=h} w_{f-1}x^{h-f}\Big| = w\,V^{(m)}(x) - \mathfrak{V}^{(m)}(x) \quad (h=0,\,1,\,\dots\,m).$$

Setzt man hierin:

$$w = \frac{\mathfrak{V}(x)}{V(x)} = \sum_{r=1}^{r=\infty} w_{r-1}x^{-r},$$

so wird in der Determinante auf der linken Seite das letzte Element gleich der unendlichen Reihe:

$$\sum_{r=h+1}^{r=\infty} w_{r-1}x^{h-r} \qquad \text{oder} \qquad \sum_{t=0}^{t=\infty} w_{h+t}x^{-t-1},$$

und da das Aggregat der ersten m Glieder dieser Reihe, als lineare Function der ersten m Determinanten-Elemente:

$$w_h,\ w_{h+1},\ \dots\ w_{h+m-1},$$

weggelassen werden kann, so resultirt die Gleichung:

$$(\mathfrak{D}'.) \qquad \mathfrak{V}(x)\,V^{(m)}(x) - \mathfrak{V}^{(m)}(x)\,V(x) = V(x)\cdot\Big|w_h,\ w_{h+1},\ \dots\ w_{h+m-1},\ \sum_{t=m}^{t=\infty} w_{h+t}x^{-t-1}\Big| \qquad (h=0,\,1,\,\dots\,m).$$

Der Ausdruck auf der linken Seite ist eine *ganze* Function von x; der Ausdruck auf der rechten Seite enthält offenbar keine höhere Potenz von x als x^{n-m-1}, diese aber mit dem Coefficienten:

$$|w_{h+k}| \qquad (h,\,k=0,\,1,\,\dots\,m)$$

multiplicirt, der Ausdruck muss daher eine ganze Function $(n-m-1)^{\text{ten}}$ Grades sein. Bezeichnet man sie mit $W^{(n-m-1)}(x)$, so ist:

$$(\mathfrak{E}_1.) \qquad \mathfrak{V}(x)\,V^{(m)}(x) - \mathfrak{V}^{(m)}(x)\,V(x) = W^{(n-m-1)}(x),$$

also auch, wenn man hierin $m-1$ an Stelle von m nimmt:

$$(\mathfrak{E}_0.) \qquad \mathfrak{V}(x)\,V^{(m-1)}(x) - \mathfrak{V}^{(m-1)}(x)\,V(x) = W^{(n-m)}(x),$$

und aus diesen beiden Gleichungen resultiren endlich mit Berücksichtigung der Gleichung ($\mathfrak{B}.$) die Relationen:

$$(\mathfrak{E}.) \qquad \begin{cases} \mathfrak{V}^{(m)}(x)\,W^{(n-m)}(x) - \mathfrak{V}^{(m-1)}(x)\,W^{(n-m-1)}(x) = V_m^2\,\mathfrak{V}(x), \\ V^{(m)}(x)\,W^{(n-m)}(x) - V^{(m-1)}(x)\,W^{(n-m-1)}(x) = V_m^2\,V(x). \end{cases}$$

Die hier gegebene Entwickelung findet sich, ihrem wesentlichen Inhalte nach, schon in meinem Aufsatze „Zur Theorie der Elimination einer

Variabeln aus zwei algebraischen Gleichungen", welcher im Monatsberichte der Berliner Akademie der Wissenschaften vom Juni 1881 abgedruckt ist[1]). Doch waren hier einige formale Modificationen nöthig, um die folgenden Ausführungen daran knüpfen zu können.

§ 2.

Aus den beiden mit (E.) bezeichneten Relationen erhellt unmittelbar die Aequivalenz der beiden Divisoren- oder Modulsysteme:

$$\left(V_m^2\,\mathfrak{V}(x),\quad V_m^2\,V(x),\quad W^{(n-m-1)}(x)\right),$$

$$\left(\mathfrak{V}^{(m)}(x)\,W^{(n-m)}(x),\quad V^{(m)}(x)\,W^{(n-m)}(x),\quad W^{(n-m-1)}(x)\right),$$

deren Elemente ganze Grössen des natürlichen Rationalitätsbereichs:

$$(\mathfrak{v}_0,\ \mathfrak{v}_1,\ \ldots\ \mathfrak{v}_{n-1},\quad v_0,\ v_1,\ \ldots\ v_{n-1},\ x)$$

sind. In dem letzteren der beiden Systeme kann aber noch das Element $V_m^2\,W^{(n-m)}(x)$ hinzugefügt werden, da es sich gemäss der Relation (B.) als ganze homogene lineare Function der beiden ersten Elemente desselben Systems darstellen lässt. Es resultirt daher die fundamentale Aequivalenz:

$$(\mathfrak{F}.)\quad \begin{cases} \left(V_m^2\,\mathfrak{V}(x),\quad V_m^2\,V(x),\quad W^{(n-m-1)}(x)\right) \\ \sim \left(V_m^2\,W^{(n-m)}(x),\quad \mathfrak{V}^{(m)}(x)\,W^{(n-m)}(x),\quad V^{(m)}(x)\,W^{(n-m)}(x),\quad W^{(n-m-1)}(x)\right), \end{cases}$$

und die Elemente dieser beiden einander äquivalenten Divisorensysteme sind folgendermaassen definirt:

[1]) Band II S. 113—192 dieser Ausgabe. H.

$$\mathfrak{V}(x)=\sum_{h=0}^{h=n-1}\mathfrak{v}_h x^h,\qquad V(x)=x^n+\sum_{h=0}^{h=n-1}v_h x^h,$$

$$V_m=\left|\,w_{i+k}\,\right|,\qquad V^{(m)}(x)=\left|\,w_{i+k}x-w_{i+k+1}\,\right|\qquad (i,\ k=0,\ 1,\ \ldots\ m-1),$$

$$-\mathfrak{V}^{(m)}(x)=\begin{vmatrix} 0, & w_0, & w_1, & \ldots & w_{m-1} \\ w_0, & w_0x-w_1, & w_1x-w_2, & \ldots & w_{m-1}x-w_m \\ w_1, & w_1x-w_2, & w_2x-w_3, & \ldots & w_mx-w_{m+1} \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ w_{m-1}, & w_{m-1}x-w_m, & w_mx-w_{m+1}, & \ldots & w_{2m-2}x-w_{2m-1} \end{vmatrix},$$

$$W^{(n-m-1)}(x)=\begin{vmatrix} \mathfrak{V}(x), & w_0, & w_1, & \ldots & w_{m-1} \\ w_0V(x), & w_0x-w_1, & w_1x-w_2, & \ldots & w_{m-1}x-w_m \\ w_1V(x), & w_1x-w_2, & w_2x-w_3, & \ldots & w_mx-w_{m+1} \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ w_{m-1}V(x), & w_{m-1}x-w_m, & w_mx-w_{m+1}, & \ldots & w_{2m-2}x-w_{2m-1} \end{vmatrix}.$$

Die Function $W^{(n-m-1)}(x)$ ist ferner gemäss den Gleichungen (D'.) und ($\mathfrak{E}_1$.) auch durch die Gleichung:

$$W^{(n-m-1)}(x)=V(x)\sum_{t=m}^{t=\infty}\left|\,w_h,\ w_{h+1},\ \ldots\ w_{h+m-1},\ w_{h+t}\,\right|x^{-t-1}\qquad (h=0,\ 1,\ \ldots\ m)$$

bestimmt, so dass also, wenn man zur Abkürzung die Determinante:

$$\left|\,w_{h+k}\,\right|\qquad \begin{pmatrix} h=0,\ 1,\ \ldots\ m-1,\ m \\ k=0,\ 1,\ \ldots\ m-1,\ t \end{pmatrix}$$

durch $V_{m,t}$ bezeichnet:

$$W^{(n-m-1)}(x)=\sum_{g=1}^{g=n-m}x^{g-1}\sum_{t=m}^{t=n-g}v_{g+t}\,V_{m,t}$$

wird. In diesem Ausdrucke von $W^{(n-m-1)}(x)$, in welchem übrigens $v_n = 1$ zu setzen ist, wird es evident, dass die Congruenz:

$$W^{(n-m-1)}(x) \equiv 0 \quad (\text{modd. } V_{m,m},\ V_{m,m+1},\ \dots\ V_{m,n-1})$$

besteht. Man kann daher in der Aequivalenz ($\mathfrak{F}$.) auf beiden Seiten das Element $W^{(n-m-1)}(x)$ durch die $n-m$ Elemente $V_{m,m}$, $V_{m,m+1}$, $\dots$ $V_{m,n-1}$ ersetzen, da überhaupt aus einer Aequivalenz zweier Modulsysteme:

$$(M_0,\ M_1,\ M_2, \dots) \sim (M_0',\ M_1',\ M_2', \dots),$$

verbunden mit den Congruenzen:

$$M_0 \equiv 0, \quad M_0' \equiv 0 \quad (\text{modd. } \mathfrak{M}_1,\ \mathfrak{M}_2, \dots)$$

die Congruenzen:

$$\begin{aligned} M_k &\equiv 0 \quad (\text{modd. } \mathfrak{M}_1,\ \mathfrak{M}_2, \dots M_1',\ M_2', \dots) \\ M_k' &\equiv 0 \quad (\text{modd. } \mathfrak{M}_1,\ \mathfrak{M}_2, \dots M_1,\ M_2, \dots) \end{aligned} \qquad (k=1, 2, \dots)$$

folgen, und hiernach auch die Aequivalenz:

$$(\mathfrak{M}_1,\ \mathfrak{M}_2, \dots M_1,\ M_2, \dots) \sim (\mathfrak{M}_1,\ \mathfrak{M}_2, \dots M_1',\ M_2', \dots)$$

besteht. Es resultirt daher eine zweite fundamentale Aequivalenz:

$$(\mathfrak{G}.) \quad \begin{cases} \left(V_m^2 \mathfrak{B}(x),\ V_m^2 V(x),\ V_{m,m},\ V_{m,m+1}, \dots V_{m,n-1}\right) \sim \\ \left(V_m^2 W^{(n-m)}(x),\ \mathfrak{B}^{(m)}(x) W^{(n-m)}(x),\ V^{(m)}(x) W^{(n-m)}(x),\ V_{m,m},\ V_{m,m+1}, \dots V_{m,n-1}\right), \end{cases}$$

und die Folgerungen, welche sich daraus ziehen lassen, bilden den Hauptzweck der vorstehenden Entwickelungen. Doch sollen zuvörderst einige Bemerkungen über das Modulsystem:

$$(V_{m,m},\ V_{m,m+1}, \dots V_{m,n-1})$$

daran geknüpft werden.

§ 3.

Da die mit $V_{m,t}$ bezeichneten ganzen Functionen der Variabeln $\mathfrak{v}$ und v durch die Gleichung:

$$V_{m,t} = |\, w_{h+k} \,| \qquad \begin{pmatrix} h=0, 1, \dots m-1, m \\ k=0, 1, \dots m-1, t \end{pmatrix}$$

oder:

$$V_{m,t} = |\, w_h,\ w_{h+1}, \dots w_{h+m-1},\ w_{h+t} \,| \qquad (h=0, 1, \dots m-1, m)$$

bestimmt sind, und für die Grössen w gemäss ihrer Definition als Entwickelungscoefficienten die Relationen:

$$-w_{h+t} = v_{n-1} w_{h+t-1} + v_{n-2} w_{h+t-2} + \cdots + v_0 w_{h+t-n} \qquad (t \geq n)$$

bestehen, so sind die Functionen $V_{m,t}$ durch die Recursionsformel:

$$-V_{m,t} = v_{n-1} V_{m,t-1} + v_{n-2} V_{m,t-2} + \cdots + v_0 V_{m,t-n} \qquad (t \geq n)$$

mit einander verbunden. Es ist daher für $t \geq n$:

$$(\mathfrak{H}^0.) \qquad V_{m,t} \equiv 0 \quad (\text{modd. } V_{m,m},\ V_{m,m+1}, \dots V_{m,n-1});$$

diese Congruenz besteht aber auch für $t = m,\ m+1, \dots n-1$ und auch für $t = 0, 1, \dots m-1$, da für diese letzteren m Werthe $V_{m,t} = 0$ wird. Das Modulsystem:

$$(V_{m,m},\ V_{m,m+1},\ \dots\ V_{m,n-1})$$

ist also dem Modulsysteme:

$$(V_{m,0},\ V_{m,1},\ V_{m,2},\ \dots\ V_{m,r})$$

aequivalent, wenn darin für r irgend eine Zahl, die grösser als $n-1$ ist, genommen wird, und es kann deshalb auch die Aequivalenz:

(§.) $(V_{m,m},\ V_{m,m+1},\ \dots\ V_{m,n-1}) \sim (V_{m,0},\ V_{m,1},\ V_{m,2},\ \dots\ V_{m,m},\ V_{m,m+1},\ \dots \text{ in inf.})$

aufgestellt werden.

Da nun oben $W^{(n-m-1)}(x)$ durch die Gleichung:

$$W^{(n-m-1)}(x) = V(x)\sum_{t=m}^{t=\infty} |\, w_h,\ w_{h+1},\ \dots\ w_{h+m-1},\ w_{h+t}\,|\, x^{-t-1} \qquad (h=0,\ 1,\ \dots\ m)$$

bestimmt worden ist, so ist, wenn unter u eine Unbestimmte (*indeterminata*) verstanden wird:

$$\frac{W^{(n-m-1)}(u^{-1})}{V(u^{-1})} = \sum_{t=m}^{t=\infty} V_{m,t}\, u^{t+1};$$

der Quotient:

$$\frac{W^{(n-m-1)}(u^{-1})}{V(u^{-1})}$$

stellt daher — im Sinne des § 22 meiner Festschrift zu Herrn *Kummer*'s Doctorjubiläum[1]) — eine „Form" dar, welche dem Modulsysteme:

$$(V_{m,m},\ V_{m,m+1},\ \dots\ V_{m,n-1})$$

entspricht und auch an dessen Stelle eintreten kann. So kann z. B. das, was die obige Congruenz:

[1]) Band II S. 342 flgde. dieser Ausgabe. H.

$$W^{(n-m-1)}(x) \equiv 0 \pmod{V_{m,m},\ V_{m,m+1},\ \dots\ V_{m,n-1}}$$

besagt, auch dadurch ausgedrückt werden, dass die Form:

$$W^{(n-m-1)}(x) \text{ als die Form } \frac{W^{(n-m-1)}(u^{-1})}{V(u^{-1})} \text{ „}\textit{enthaltend}\text{"}$$

bezeichnet wird, und in dieser Fassung tritt das Resultat gewissermaassen in Evidenz.

Dass das Divisorensystem $(V_{m,m},\ V_{m,m+1},\ \dots\ V_{m,n-1})$ ein System $(n-m)^{\text{ter}}$ Stufe ist, lässt sich leicht erkennen, wenn man die Grössen $w_0,\ w_1,\ \dots\ w_{2n-1}$ an Stelle der Grössen $\mathfrak{v}_0,\ \mathfrak{v}_1,\ \dots\ \mathfrak{v}_{n-1},\ v_0,\ v_1,\ \dots\ v_{n-1}$ als unabhängige Variable auffasst. Denn das letzte Element der mit $V_{m,t}$ bezeichneten Determinante ist w_{m+t}, und es ist daher:

$V_{m,m}$ eine lineare Function von w_{2m}, deren Coefficienten nur $w_0,\ w_1,\ \dots\ w_{2m-1}$ enthalten,

$V_{m,m+1}$ eine lineare Function von w_{2m+1}, deren Coefficienten nur $w_0,\ w_1,\ \dots\ w_{2m}$ enthalten,

u. s. f. Die Resultante der Elimination von $w_{2m},\ w_{2m+1},\ \dots\ w_{m+n-1}$ aus den Gleichungen:

$$V_{m,m} = 0, \quad V_{m,m+1} = 0, \dots\ V_{m,n-1} = 0$$

ist also nicht identisch gleich Null.

Man kann nun in der That die $2n$ Grössen $w_0,\ w_1,\ \dots\ w_{2n-1}$ an Stelle der $2n$ Grössen:

$$\mathfrak{v}_0,\ \mathfrak{v}_1,\ \dots\ \mathfrak{v}_{n-1};\quad v_0,\ v_1,\ \dots\ v_{n-1}$$

als unabhängige Variable auffassen, da sich die letzteren durch die ersteren

rational ausdrücken lassen. Gemäss der Definition der Grössen w ist nämlich für $h = 0, 1, 2, \ldots n-1$:

$$w_h + v_{n-1} w_{h-1} + v_{n-2} w_{h-2} + \cdots + v_{n-h} w_0 = \mathfrak{v}_{n-h-1},$$

und es können hiernach die ersten n Grössen w an Stelle der n Grössen $\mathfrak{v}$ eingeführt werden. Die n Grössen $v_0, v_1, \ldots v_{n-1}$ bestimmen sich alsdann aus den $2n$ Grössen $w_0, w_1, \ldots w_{2n-1}$ mittels der n Gleichungen:

$$w_{n+h} + v_{n-1} w_{n+h-1} + v_{n-2} w_{n+h-2} + \cdots + v_0 w_h = 0 \qquad (h = 0, 1, 2, \ldots n-1).$$

Eben dieselbe Bestimmung der Grössen w aus den Grössen $\mathfrak{v}$ und v ergiebt sich direct aus den obigen Formeln ($\mathfrak{D}'$.) und ($\mathfrak{E}$.), wenn man darin $m = n$ nimmt. Alsdann muss nämlich der Ausdruck auf der rechten Seite gleich Null werden, und es kommt:

$$\mathfrak{V}(x) V^{(n)}(x) = \mathfrak{V}^{(n)}(x) V(x),$$

also:

$$V(x) = \frac{V^{(n)}(x)}{V_n}, \quad \mathfrak{V}(x) = \frac{\mathfrak{V}^{(n)}(x)}{V_n},$$

und diese beiden Gleichungen liefern unmittelbar $v_0, v_1, \ldots v_{n-1}$, $\mathfrak{v}_0, \mathfrak{v}_1, \ldots \mathfrak{v}_{n-1}$ als rationale Functionen der Grössen $w_0, w_1, \ldots w_{2n-1}$.

Bedeutet r eine der Zahlen $0, 1, 2, \ldots n-m$, so lässt sich die Determinante $(m+r+1)^{\text{ter}}$ Ordnung:

$$|w_{p+q}| \qquad (p, q = 0, 1, 2, \ldots m+r)$$

als ganze Function von $w_0, w_1, \ldots w_{2m+r-1}$ und $V_{m,m}, V_{m,m+1}, \ldots V_{m,m+2r}$ darstellen. Ist nämlich:

$$|w_h, w_{h+1}, \ldots w_{h+m-1}, z^{(m-h)}| = \sum_h z^{(h)} V_m^{(h)} \qquad (h = 0, 1, 2, \ldots m),$$

wo $z^0, z', z'', \ldots z^{(m)}$ unbestimmte Variable bedeuten, so sind $V_m^{(0)}, V_m', V_m'', \ldots V_m^{(m)}$ Determinanten m^{ter} Ordnung, und zwar ist $V_m^{(0)}$ genau diejenige, welche oben mit V_m bezeichnet worden ist. Hiernach wird:

($\mathfrak{F}$.) $$V_{m,t} = \sum_h w_{m-h+t} V_m^{(h)} \qquad (h = 0, 1, 2, \ldots m),$$

und wenn man nun jede der $r+1$ letzten Horizontalreihen in der Determinante:

$$|w_{p+q}| \qquad (p, q = 0, 1, 2, \ldots m+r)$$

mit $V_m^{(0)}$ multiplicirt und alsdann derselben die nächstvorhergehende, mit V_m' multiplicirt, die zweitvorhergehende, mit V_m'' multiplicirt, u. s. f. hinzufügt, so treten an Stelle der $r+1$ letzten Horizontalreihen:

$$w_p, \; w_{p+1}, \; w_{p+2}, \; \ldots \; w_{p+m+r} \qquad (p = m, m+1, \ldots m+r)$$

die folgenden:

$$V_{m,p-m}, \; V_{m,p-m+1}, \; V_{m,p-m+2}, \; \ldots \; V_{m,p+r} \qquad (p = m, m+1, \ldots m+r).$$

Dabei ist zu bemerken, dass $V_{m,t} = 0$ ist, wenn $t < m$ ist, und dass in dem von den Horizontalreihen der Grössen $V_{m,t}$ gebildeten Rechteck nur die Ecke rechts Grössen $V_{m,t}$ enthält, in denen $t \geqq m+r$ ist. Alle diese Grössen füllen ein rechtwinkliges Dreieck aus, dessen Hypotenuse $r+1$ Grössen $V_{m,m+r}$ enthält. Betrachtet man also die aus den m Horizontalreihen:

$$w_h, \; w_{h+1}, \; \ldots \; w_{h+m+r} \qquad (h = 0, 1, \ldots m-1)$$

und aus den $r+1$ Horizontalreihen:

$$V_{m,k}, \; V_{m,k+1}, \; \ldots \; V_{m,k+m+r} \qquad (k = 0, 1, \ldots r)$$

gebildete Determinante nur:

modulis: $V_{m,m},\ V_{m,m+1},\ \cdots\ V_{m,m+r-1}$,

so reducirt sie sich auf:

$$|w_{h+k}| \cdot V_{m,m+r}^{r+1} \qquad (h, k = 0, 1, \ldots m-1).$$

Es besteht daher die Congruenz:

$$|w_{p+q}| \cdot V_m^{r+1} \equiv |w_{h+k}| \cdot V_{m,m+r}^{r+1} \quad (\text{modd. } V_{m,m},\ V_{m,m+1},\ \cdots\ V_{m,m+r-1})$$
$$(p, q = 0, 1, 2, \ldots m+r;\ h, k = 0, 1, 2, \ldots m-1),$$

oder wenn zur Abkürzung:

$$|w_{p+q}| = W_{m+r} \qquad (p, q = 0, 1, 2, \ldots m+r)$$

und wie oben:

$$|w_{h+k}| = V_m \qquad (h, k = 0, 1, 2, \ldots m-1)$$

gesetzt wird:

(ℜ.) $$V_m^{r+1} W_{m+r} \equiv V_m V_{m,m+r}^{r+1} \quad (\text{modd. } V_{m,m},\ V_{m,m+1},\ \cdots\ V_{m,m+r-1}).$$

Für $r = 0$ wird die Determinante W_{m+r}, ihrer Definition nach, mit $V_{m,m}$ identisch, d. h. es ist $W_m = V_{m,m}$, und die Congruenz (ℜ.) zeigt also, dass das Modulsystem:

$$(V_{m,m},\ V_{m,m+1},\ \cdots\ V_{m,n-1})$$

in dem Modulsysteme:

$$(V_m W_m,\ V_m^2 W_{m+1},\ V_m^3 W_{m+2},\ \cdots\ V_m^{n-m} W_{n-1})$$

enthalten ist.

Es lässt sich aber auch andererseits aus der Congruenz (ℜ.) erschliessen, dass das Modulsystem $(W_m,\ W_{m+1},\ W_{m+2},\ \cdots W_{n-1})$ in einem Modulsysteme enthalten ist, dessen Elemente Potenzen von V_m, multiplicirt mit Potenzen von $V_{m,m},\ V_{m,m+1},\ \cdots V_{m,n-1}$, sind. Erstens ist nämlich:

$$V_{m,m} = W_m;$$

ferner ergiebt die Congruenz (ℜ.) für $r = 1$, dass:

$$V_m V_{m,m+1}^2 \equiv 0 \quad (\text{modd. } W_m,\ W_{m+1})$$

ist, und alsdann für $r = 2$, dass:

$$V_m V_{m,m+2}^3 = V_m^3 W_{m+2} + G V_{m,m+1} + G_1 W_m$$

wird, wo G und G_1 ganze ganzzahlige Functionen der Grössen w bedeuten. Erhebt man die Ausdrücke auf beiden Seiten der Gleichung zum Quadrat, so erhält man die Congruenz:

$$V_m^3 V_{m,m+2}^6 \equiv 0 \quad (\text{modd. } W_m,\ W_{m+1},\ W_{m+2}).$$

Nimmt man nun an, dass in der angegebenen Weise eine Congruenz:

(ℜ'.) $$V_m^{p_r+q_r} V_{m,m+r-1}^{r q_r} \equiv 0 \quad (\text{modd. } W_m,\ W_{m+1},\ \cdots W_{m+r-1})$$

erlangt sei, so folgt aus der Congruenz (ℜ.) die Gleichung:

$$V_m^{p_{r+1}} (V_m V_{m,m+r}^{r+1})^{q_{r+1}} = V_m^{p_{r+1}} (V_m^{r+1} W_{m+r} + G_1 V_{m,m+r-1} + G_2 V_{m,m+r-2} + \cdots + G_r V_{m,m})^{q_{r+1}}$$

für beliebige ganze Zahlen p_{r+1}, q_{r+1}. Nimmt man diese durch die Recursionsformeln:

$$q_{r+1} = r q_r + (r-1) q_{r-1} + \cdots + 3 q_3 + 2 q_2 - r + 2,$$
$$p_{r+1} = q_r + q_{r-1} + \cdots + q_3 + q_2$$

bestimmt an, so ist jedes der bei der Entwicklung der $(q_{r+1})^{\text{ten}}$ Potenz rechts vorkommenden Glieder:

$$V_m^{p_{r+1}} V_{m,m+r-1}^{h_r} V_{m,m+r-2}^{h_{r-1}} \cdots V_{m,m+1}^{h_2}$$

durch ein Product:

$$V_m^{p_k+q_k} V_{m,m+k-1}^{kq_k} \qquad (2 \leq k \leq r)$$

theilbar. Denn erstens ist für jeden der $r-1$ Werthe von k:

$$p_k + q_k \leq p_{r+1},$$

und da zweitens $h_2 + h_3 + \cdots + h_r = q_{r+1}$, also:

$$\sum_{k=2}^{k=r} (h_k - kq_k) = -r+2$$

ist, so muss wenigstens für *einen* der $r-1$ Werthe von k:

$$kq_k \leq h_k$$

sein. Die Congruenz ($\mathfrak{R}'$.) gilt hiernach auch, wenn man darin $r+1$ statt r nimmt, und sie gilt also für *alle* Werthe $r = 1, 2, \ldots n-m$. Es ist daher in der That das Modulsystem:

$$(W_m,\ W_{m+1},\ W_{m+2},\ \cdots W_{n-1})$$

in dem Modulsysteme:

$$(\ldots\ V_m^{t_r} V_{m,m+r-1}^{rq_r}, \ldots) \qquad (r = 1, 2, \ldots n-m)$$

enthalten, wenn die Zahlen q_r, t_r durch die Gleichungen:

$$q_1 = 1, \quad q_{r+1} - 1 = \sum_{k=1}^{k=r} (kq_k - 1), \quad t_r + 1 = \sum_{k=1}^{k=r} q_k \qquad (r = 1, 2, \ldots n-m)$$

bestimmt werden.

Die hier entwickelten Beziehungen zwischen den Determinanten $V_{m,s}$ und W_{m+r} können in folgende Congruenzen zusammengefasst werden:

$$(\mathfrak{R}_1.) \qquad V_m^r W_{m+r-1} \equiv 0 \pmod{V_{m,m},\ V_{m,m+1}, \ldots V_{m,n-1}}$$

$$(\mathfrak{R}_2.) \qquad V_m^{t_r} V_{m,m+r-1}^{rq_r} \equiv 0 \pmod{W_m,\ W_{m+1},\ \ldots\ W_{n-1}} \qquad (r = 1, 2, \ldots n-m).$$

Es geht aus ihnen hervor, dass

> einerseits das Modulsystem $(V_{m,m},\ V_{m,m+1}, \ldots V_{m,n-1})$ in dem mit V_m^{n-m} multiplicirten Modulsysteme $(W_m,\ W_{m+1}, \ldots\ W_{n-1})$, andererseits dieses letztere in einer *Potenz* des mit V_m multiplicirten ersteren enthalten ist, wenn der Exponent genügend gross, z. B. gleich
>
> $$m - n + 1 + q_1 + 2q_2 + 3q_3 + \cdots + (n-m)q_{n-m}$$
>
> angenommen wird.

Jene merkwürdige Aequivalenz der beiden Systeme von Bedingungen:

$$V_m \gtrless 0, \quad V_{m,m} = 0, \quad V_{m,m+1} = 0, \ldots\ V_{m,n-1} = 0,$$

$$V_m \gtrless 0, \quad W_m = 0, \quad W_{m+1} = 0, \ldots\ W_{n-1} = 0,$$

welche ich schon im art. VII meines oben citirten Aufsatzes*) nachgewiesen

*) Monatsbericht der hiesigen Akademie vom Juni 1881[1]).

[1]) Band II S. 146 flgde. dieser Ausgabe. H.

habe, tritt hier in Evidenz. Aber die Congruenzen $(\mathfrak{R}_{1.})$, $(\mathfrak{R}_{2.})$ sind nicht nur die wahre Quelle für die angegebene Aequivalenz, sondern sie ergeben auch allgemeinere Resultate, welche im Folgenden entwickelt werden sollen.

§ 4.

Die im vorigen Paragraphen entwickelte Gleichung $(\overline{\mathfrak{H}}_{.})$:

$$V_{m,\,t} = \sum_{h} w_{m-h+t}\, V_m^{(h)} \qquad (h=0,\,1,\,2,\,\ldots\,m)$$

lässt sich, da $V_m^{(0)} = V_m$ ist, in folgender Weise darstellen:

$$w_s V_m + w_{s-1} V_m^{(1)} + w_{s-2} V_m^{(2)} + \cdots + w_{s-m} V_m^{(m)} = V_{m,\,s-m} \qquad (s \geqq m).$$

Da nun, gemäss der Congruenz $(\mathfrak{H}^0_{.})$ im § 3, jede Determinante $V_{m,\,s-m}$ das Modulsystem $(V_{m,\,m},\ V_{m,\,m+1},\ \ldots\ V_{m,\,n-1})$ enthält, so besteht — im Sinne der Congruenz für dieses Modulsystem — zwischen den Grössen w eine „lineare Recursionsformel m^{ter} Ordnung", nämlich*):

$$w_s V_m + w_{s-1} V_m^{(1)} + w_{s-2} V_m^{(2)} + \cdots + w_{s-m} V_m^{(m)} \equiv 0 \pmod{V_{m,\,m},\ V_{m,\,m+1},\ \ldots\ V_{m,\,n-1}}.$$

In dem Systeme der Grössen:

$$w_{p+q}\, V_m^{q-m+1} \qquad (p,\ q=0,\,1,\,2,\,\ldots),$$

oder genauer in dem Systeme:

*) Vgl. die Definitionen im art. VII meines mehrfach citirten, im Monatsberichte der hiesigen Akademie vom Juni 1881 abgedruckten Aufsatzes[1]).

[1]) Band II S. 146 f. dieser Ausgabe. H.

$$\begin{array}{llllll}
w_0, & w_1, & w_2, & \ldots\ w_{m-1}, & w_m V_m, & w_{m+1} V_m^2, \quad w_{m+2} V_m^3, \quad \ldots \\
w_1, & w_2, & w_3, & \ldots\ w_m, & w_{m+1} V_m, & w_{m+2} V_m^2, \quad w_{m+3} V_m^3, \quad \ldots \\
w_2, & w_3, & w_4, & \ldots\ w_{m+1}, & w_{m+2} V_m, & w_{m+3} V_m^2, \quad w_{m+4} V_m^3, \quad \ldots \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot \quad \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot \quad \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot \quad \cdot
\end{array}$$

mit beliebig weit fortgesetzten Horizontal- und Vertical-Reihen ist daher *modulis* $V_{m,\,m},\ V_{m,\,m+1},\ \ldots\ V_{m,\,n-1}$ jede Verticalreihe eine lineare homogene Function der m unmittelbar vorhergehenden;

jede Determinante $(m+1)^{ter}$ Ordnung dieses Systems ist also modulis $V_{m,\,m},\ V_{m,\,m+1},\ \ldots\ V_{m,\,n-1}$ congruent Null, d. h. der Rang des Grössensystems:

$$w_{p+q}\, V_m^{q-m+1} \qquad (p,\ q=0,\,1,\,2,\,\ldots)$$

ist in Beziehung auf das aus den $n-m$ Determinanten:

$$|\, w_{h+k}\,| \qquad \begin{pmatrix} h=0,\,1,\,\ldots\,m-1,\,m \\ k=0,\,1,\,\ldots\,m-1,\,t \\ t=m,\,m+1,\,\ldots\,n-1 \end{pmatrix}$$

zu bildende Modulsystem genau gleich m.

Ferner folgt hieraus mit Hülfe der am Schlusse des vorigen Paragraphen gegebenen Entwickelungen:

dass eine Potenz jeder aus dem Grössensysteme:

$$w_{p+q} \qquad (p,\ q=0,\,1,\,2,\,\ldots)$$

zu bildenden Determinante $(m+1)^{ter}$ Ordnung, nach Multiplication mit

einer genügend hohen Potenz von V_m, modulis W_m, W_{m+1}, ... W_{n-1} congruent Null wird, also das aus den $n-m$ Hauptdeterminanten:

$$|w_{p+q}| \qquad \begin{pmatrix} p,\ q = 0,\ 1,\ 2,\ \dots\ m+r \\ r = 0,\ 1,\ 2,\ \dots\ n-m-1 \end{pmatrix}$$

zu bildende Modulsystem enthält.

Nimmt man für $\mathfrak{v}_0, \mathfrak{v}_1, \dots \mathfrak{v}_{n-1}$, $v_0, v_1, \dots v_{n-1}$ irgend welche ganze Grössen eines natürlichen Rationalitätsbereichs $(\mathfrak{R}', \mathfrak{R}'', \dots \mathfrak{R}^{(n-1)})$, so sind auch $w_0, w_1, w_2, \dots$ ganze Grössen desselben Bereichs; denn die ersten $2n$ Grössen w sind nach §§ 1 und 3 mit den Grössen $\mathfrak{v}$ und v durch die Relationen:

$$w_h + v_{n-1}w_{h-1} + v_{n-2}w_{h-2} + \cdots + v_{n-h}w_0 = \mathfrak{v}_{n-h-1} \qquad (h = 0,\ 1,\ \dots\ n-1),$$

$$w_k + v_{n-1}w_{k-1} + v_{n-2}w_{k-2} + \cdots + v_0 w_{k-n} = 0 \qquad (k = n,\ n+1,\ \dots\ 2n-1)$$

verbunden, während sich die Grössen w_{2n}, $w_{2n+1}, \dots$ alsdann durch die letztere Gleichung für $k \geq 2n$ bestimmen.

Die Determinanten $(n+1)^{\text{ter}}$ Ordnung, welche aus dem System:

$$w_{p+q} \qquad (p,\ q = 0,\ 1,\ 2,\ \dots)$$

gebildet werden können, sind sämmtlich gleich Null. Der (absolute) Rang dieses Systems ist also gleich n, wenn die Determinante n^{ter} Ordnung:

$$|w_{p+q}| \qquad (p,\ q = 0,\ 1,\ \dots\ n-1)$$

von Null verschieden ist; aber der „Rang in Beziehung auf ein Primmodulsystem" $(M', M'', M''', \dots)$ des Rationalitätsbereichs $(\mathfrak{R}', \mathfrak{R}'', \dots \mathfrak{R}^{(n-1)})$ ist gleich m, wenn m die grösste Ordnungszahl aller das Modulsystem $(M', M'', M''', \dots)$ nicht enthaltenden Determinanten ist. Da aber oben gezeigt worden ist, dass *jede* aus dem Systeme w_{p+q} zu bildende Determinante $(m+1)^{\text{ter}}$ Ordnung, nach Multiplication mit einer Potenz der Determinante V_m, das aus den

$n-m$ speciellen Determinanten $(m+1)^{\text{ter}}$ Ordnung $V_{m,m}$, $V_{m,m+1}, \dots V_{m,n-1}$ bestehende Modulsystem enthält, so genügen für die Charakterisirung der Rangzahl m die Bedingungen:

$(\mathfrak{L}.)$ V_m nicht $\equiv 0$, $V_{m,m} \equiv 0$, $V_{m,m+1} \equiv 0, \dots V_{m,n-1} \equiv 0$ (modd. $M', M'', M''', \dots$)

oder:

$(\mathfrak{L}'.)$ $|w_{g+h}|$ nicht $\equiv 0$, $|w_{i+k}| \equiv 0$ (modd. $M', M'', M''', \dots$)
$(g,\ h = 0,\ 1,\ \dots\ m-1)$, $(i = 0,\ 1,\ \dots\ m-1,\ m;\ k = 0,\ 1,\ \dots\ m-1,\ t;\ t = m,\ m+1,\ \dots\ n-1)$,

welche, vermöge der Congruenzen $(\mathfrak{R}_1.)$ und $(\mathfrak{R}_2.)$ im § 3, und weil $(M', M'', M''', \dots)$ als ein *Prim*modulsystem vorausgesetzt worden, mit den Bedingungen:

$(\mathfrak{M}.)$ V_m oder W_{m-1} nicht $\equiv 0$, $W_m \equiv 0$, $W_{m+1} \equiv 0, \dots W_{n-1} \equiv 0$
(modd. $M', M'', M''', \dots$)

oder:

$(\mathfrak{M}'.)$ $|w_{g+h}|$ nicht $\equiv 0$, $|w_{p+q}| \equiv 0$ (modd. $M', M'', M''', \dots$)
$(g,\ h = 0,\ 1,\ \dots\ m-1)$ $(p,\ q = 0,\ 1,\ 2,\ \dots\ m+r;\ r = 0,\ 1,\ 2,\ \dots\ n-m-1)$

völlig äquivalent sind. Aus diesen letzteren Bedingungen geht hervor, dass es genügt,

die Rangzahl m als die grösste Ordnungszahl aller das Modulsystem nicht enthaltenden *Haupt*determinanten:

$(\mathfrak{R}.)$ $$w_0, \quad \begin{vmatrix} w_0, & w_1 \\ w_1, & w_2 \end{vmatrix}, \quad \begin{vmatrix} w_0, & w_1, & w_2 \\ w_1, & w_2, & w_3 \\ w_2, & w_3, & w_4 \end{vmatrix}, \dots$$

zu definiren;

und dies ist wohl die einfachste Weise, den Rang eines Systems w_{p+q} in Beziehung auf irgend ein Primmodulsystem zu charakterisiren.

§ 5.

Gemäss der Aequivalenz (G.), am Schlusse des § 2, müssen Congruenzen:

$$(\mathfrak{P}.)\qquad \begin{cases} V_m^2 \mathfrak{B}(x) \equiv \mathfrak{Q}(x) W^{(n-m)}(x), \quad V_m^2 V(x) \equiv Q(x) W^{(n-m)}(x), \\ V_m^2 W^{(n-m)}(x) \equiv V_m^2 \mathfrak{P}(x)\mathfrak{B}(x) + V_m^2 P(x) V(x) \end{cases}$$

für das Modulsystem:

$$(V_{m,m},\ V_{m,m+1},\ \ldots\ V_{m,n-1})$$

bestehen, in welchen:

$$\mathfrak{P}(x),\quad \mathfrak{Q}(x),\quad P(x),\quad Q(x)$$

ganze Functionen von x bedeuten, deren Coefficienten ganze ganzzahlige Functionen der Variabeln $\mathfrak{v}$ und v sind.

Nach § 1, $(\mathfrak{E}_0.)$ und $(\mathfrak{E}.)$ kann z. B.

$$\mathfrak{P}(x) = V^{(m-1)}(x),\quad P(x) = -\mathfrak{V}^{(m-1)}(x),\quad \mathfrak{Q}(x) = \mathfrak{V}^{(m)}(x),\quad Q(x) = V^{(m)}(x)$$

genommen werden.

So wie nun überhaupt durch drei Gleichungen:

$$(\mathfrak{Q}.)\qquad \varphi(x) = f(x)g(x),\quad \psi(x) = f(x)h(x),\quad f(x) = \varphi(x)\varphi_1(x) + \psi(x)\psi_1(x),$$

in denen $f(x)$, $g(x)$, $h(x)$, $\varphi(x)$, $\varphi_1(x)$, $\psi(x)$, $\psi_1(x)$ ganze Functionen von x bedeuten,

$f(x)$ als grösster gemeinsamer Theiler von $\varphi(x)$ und $\psi(x)$

vollständig charakterisirt wird, so lässt sich auch der Inhalt jener fundamentalen Aequivalenz (G.) dahin formuliren, dass

die Function $W^{(n-m)}(x)$ den grössten gemeinsamen Theiler der beiden Functionen $V_m^2 \mathfrak{B}(x)$ und $V_m^2 V(x)$ modulis $V_{m,m}$, $V_{m,m+1}$, $\ldots$ $V_{m,n-1}$ darstellt.

Es muss sich daher bei dem Verfahren zur Aufsuchung des grössten gemeinsamen Theilers von $V(x)$ und $\mathfrak{B}(x)$ die mit $W^{(n-m)}(x)$ bezeichnete Function als solcher ergeben, wenn man bei diesem Verfahren jede ganze Function der Coefficienten $\mathfrak{v}$ und v gleich Null setzt, die sich als ganze lineare homogene Function von:

$$V_{m,m},\ V_{m,m+1},\ \ldots\ V_{m,n-1}$$

darstellen lässt, deren Coefficienten selbst ganze Functionen der Grössen $\mathfrak{v}$ und v sind.

Es seien nun, wie im vorigen Paragraphen, die Coefficienten von $\mathfrak{B}(x)$ und $V(x)$ ganze Grössen des natürlichen Rationalitätsbereichs $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$, ferner bedeute $(M', M'', M''', \ldots)$, ebenso wie dort, ein Primmodulsystem desselben Bereichs, und der Rang des aus den Entwickelungscoefficienten $w_0, w_1, w_2, \ldots$ von:

$$\frac{\mathfrak{B}(x)}{V(x)} = w_0 x^{-1} + w_1 x^{-2} + w_2 x^{-3} + \ldots$$

zu bildenden Systems:

$$\begin{array}{lll} w_0, & w_1, & w_2, \ldots \\ w_1, & w_2, & w_3, \ldots \\ w_2, & w_3, & w_4, \ldots \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{array}$$

sei in Beziehung auf das Modulsystem $(M', M'', M''', \ldots)$ gleich m. Alsdann ist dieses Modulsystem in dem Modulsysteme $(V_{m,m}, V_{m,m+1}, \ldots V_{m,n-1})$ enthalten, und die obigen Congruenzen (𝔓.) gelten daher auch *modulis* $M', M'', M''', \ldots$. Da ferner, gemäss der Charakterisirung der Rangzahl m, die Determinante V_m das Primmodulsystem $(M', M'', M''', \ldots)$ *nicht* enthält, so kann der Factor V_m^2 in der letzten der drei Gleichungen (𝔓.) weggelassen, in den beiden ersten aber durch eine in Beziehung auf das Modulsystem $(M', M'', M''', \ldots)$ primitive oder Einheits-Form E ersetzt werden.

Hiernach bestehen für das Modulsystem $(M', M'', M''', \ldots)$ Congruenzen:

$$(\mathfrak{P}.) \qquad \begin{cases} E \cdot \mathfrak{B}(x) \equiv \mathfrak{Q}(x)\, W^{(n-m)}(x), \quad E \cdot V(x) \equiv Q(x)\, W^{(n-m)}(x), \\ W^{(n-m)}(x) \equiv \mathfrak{P}(x)\mathfrak{B}(x) + P(x)\, V(x), \end{cases}$$

welche die Function $W^{(n-m)}(x)$ als grössten gemeinsamen Theiler von $\mathfrak{B}(x)$ und $V(x)$ *modulis* $M', M'', M''', \ldots$ charakterisiren. Ebenso wie aber jenes System von drei Gleichungen (𝔔.) einfach durch die Aequivalenz

$$(\varphi(x),\ \psi(x)) \sim f(x)$$

ersetzt werden kann, welche zeigt, dass das Divisorensystem $(\varphi(x),\ \psi(x))$ sich auf den einfachen Divisor $f(x)$ reduciren lässt, so kann auch der wesentliche Inhalt des Systems der drei Congruenzen (𝔓), mit Weglassung der nebensächlichen Functionen $\mathfrak{Q}(x)$, $Q(x)$, $\mathfrak{P}(x)$, $P(x)$, durch die Aequivalenz:

$$(\mathfrak{R}.) \qquad (\mathfrak{B}(x),\ V(x)) \sim W^{(n-m)}(x) \quad (\text{modd. } M', M'', M''', \ldots)$$

einfach und deutlich dargestellt werden.

In dieser Aequivalenz ist der Zielpunkt der vorstehenden Auseinandersetzungen enthalten, nämlich die *Bestimmung des grössten gemeinsamen Theilers zweier ganzen Functionen* $\mathfrak{B}(x)$ *und* $V(x)$ *für irgend ein Primmodulsystem* $(M', M'', M''', \ldots)$. Denn mit Hülfe der Entwickelungscoefficienten $w_0, w_1, w_2, \ldots$ von:

$$\frac{\mathfrak{B}(x)}{V(x)} = w_0 x^{-1} + w_1 x^{-2} + w_2 x^{-3} + \cdots$$

lässt sich der grösste gemeinsame Theiler von $\mathfrak{B}(x)$ und $V(x)$, welcher oben mit $W^{(n-m)}(x)$ bezeichnet worden ist, als ganze Function $(n-m)^{\text{ten}}$ Grades von x, nach § 2 durch:

$$\sum_{h=0}^{h=n-m} x^h \sum_{r=h+m}^{r=n} v_r \left| w_{i+k} \right| \qquad \left(\begin{smallmatrix} i=0,\ 1,\ \ldots\ m-2,\ m-1 \\ k=0,\ 1,\ \ldots\ m-2,\ r-h-1 \end{smallmatrix}\right)$$

oder durch die Determinante:

$$\begin{vmatrix} \mathfrak{B}(x), & w_0, & w_1, & \ldots & w_{m-2} \\ w_0 V(x), & w_0 x - w_1, & w_1 x - w_2, & \ldots & w_{m-2} x - w_{m-1} \\ w_1 V(x), & w_1 x - w_2, & w_2 x - w_3, & \ldots & w_{m-1} x - w_m \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ w_{m-2} V(x), & w_{m-2} x - w_{m-1}, & w_{m-1} x - w_m, & \ldots & w_{2m-4} x - w_{2m-3} \end{vmatrix}$$

darstellen, und die Zahl m ist hierbei durch den *Rang* bestimmt, welcher dem Grössensystem:

$$\begin{array}{lllll} w_0, & w_1, & w_2, & \ldots \\ w_1, & w_2, & w_3, & \ldots \\ w_2, & w_3, & w_4, & \ldots \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{array}$$

in Beziehung auf das Modulsystem $(M', M'', M''', \ldots)$ zukommt.

Die Bestimmung des grössten gemeinsamen Theilers, den zwei Functionen $\mathfrak{B}(x)$ und $V(x)$ *an sich*, d. h. ohne Beziehung auf irgend ein bestimmtes Modulsystem haben, kann als ein specieller Fall des oben behandelten

Problems aufgefasst werden. Denn wenn man dem Rationalitätsbereich $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$, welchem die Coefficienten von $\mathfrak{B}(x)$ und $V(x)$ angehören, eine neue Variable $\mathfrak{R}$ hinzufügt und diese selbst an Stelle des Modulsystems $(M', M'', M''', \ldots)$ als Modul einführt, so besteht die Aequivalenz $(\overline{\mathfrak{R}})$ offenbar nicht nur *mod.* $\mathfrak{R}$, sondern auch *an sich*, da die Coefficienten der Functionen $\mathfrak{B}(x)$, $V(x)$ und $W^{(n-m)}(x)$ von $\mathfrak{R}$ unabhängig sind und also jede ganze Function dieser Coefficienten, welche *mod.* $\mathfrak{R}$ congruent Null ist, auch *gleich* Null sein muss.

§ 6.

Für den einfachen Fall des absoluten Rationalitätsbereichs $\mathfrak{R} = 1$ sind $\mathfrak{v}_0, \mathfrak{v}_1, \ldots v_0, v_1, \ldots w_0, w_1, \ldots$ ganze Zahlen, und an die Stelle des Primmodulsystems $(M', M'', M''', \ldots)$ tritt eine gewöhnliche Primzahl p. Ist alsdann die Determinante m^{ter} Ordnung die letzte in der Reihe der Hauptdeterminanten:

$$w_0, \quad \begin{vmatrix} w_0, & w_1 \\ w_1, & w_2 \end{vmatrix}, \quad \begin{vmatrix} w_0, & w_1, & w_2 \\ w_1, & w_2, & w_3 \\ w_2, & w_3, & w_4 \end{vmatrix}, \ldots,$$

deren Werth nicht durch p theilbar ist, so ist (nach § 4) der Rang des Systems der Zahlen w_{p+q} in Beziehung auf den Modul p genau gleich m, und die beiden ganzen ganzzahligen Functionen von x:

$$\mathfrak{v}_0 + \mathfrak{v}_1 x + \mathfrak{v}_2 x^2 + \cdots + \mathfrak{v}_{n-1} x^{n-1}, \quad v_0 + v_1 x + v_2 x^2 + \cdots + v_{n-1} x^{n-1} + x^n$$

haben, *modulo* p betrachtet, einen grössten gemeinsamen Theiler vom Grade $n - m$.

Nimmt man speciell $n = p - 1$, $v_0 = -1$, $v_1 = 0$, $v_2 = 0, \ldots v_{n-1} = 0$, so ist:

$$w_{h+nk} = \mathfrak{v}_{n-h-1}, \quad \text{also} \quad w_{h+nk} = w_h \qquad \begin{pmatrix} h=0, 1, \ldots n-1 \\ k=0, 1, \ldots \text{in inf.} \end{pmatrix},$$

und es wird dann durch die obigen Entwickelungen der grösste gemeinsame Theiler der beiden ganzen ganzzahligen Functionen von x:

$$w_0 x^{p-2} + w_1 x^{p-3} + w_2 x^{p-4} + \cdots + w_{p-3} x + w_{p-2} \quad \text{und} \quad x^{p-1} - 1$$

modulo p bestimmt. Da dieser aber nichts Anderes ist als das Product:

$$(x - x_1)(x - x_2) \cdots (x - x_{n-m}),$$

wenn $x_1, x_2, \ldots x_{n-m}$ die sämmtlichen, unter einander und von Null verschiedenen Wurzeln der Congruenz:

$$(\mathfrak{S}.) \qquad w_0 x^{p-2} + w_1 x^{p-3} + \cdots + w_{p-3} x + w_{p-2} \equiv 0 \pmod{p}$$

bedeuten, so ist es eben dieses Product, welches nach § 5 durch den Quotienten zweier Determinanten m^{ter} Ordnung:

$$\frac{1}{|w_{g+h}|} \cdot \left| w_g, w_{g+1}, \ldots w_{g+m-2}, w_{g+m-1} x^{n-m} + w_{g+m} x^{n-m-1} + \cdots + w_{g+n-2} x + w_{g+n-1} \right|_{(g,\, h = 0, 1, 2, \ldots m-1)}$$

(mod. p) dargestellt wird, und es sind die Bedingungen für das Vorhandensein von genau $n - m$ unter einander und von Null verschiedenen Congruenzwurzeln, welche dadurch ausgedrückt werden, dass die Determinante:

$$(\mathfrak{S}'.) \qquad |w_{i+k}| \qquad (i, k = 0, 1, 2, \ldots r)$$

für $r = n - 1, n - 2, \ldots m$ durch p theilbar, aber für $r = m - 1$ *nicht* durch p theilbar sein soll.

Gemäss § 4 $(\mathfrak{L}'.)$ können diese Bedingungen durch die folgenden ersetzt werden:

$(\mathfrak{S}''.)$ $\quad |w_{g+h}| \text{ nicht } \equiv 0, \qquad |w_{i+k}| \equiv 0 \pmod{p}.$

$(g, h = 0, 1, \ldots m-1) \qquad (i = 0, 1, \ldots m-1, m; k = 0, 1, \ldots m-1, t; t = m, m+1, \ldots n-1).$

Mit diesen sind aber, wie im § 4 gezeigt worden ist, zugleich die Bedingungen dafür erfüllt, dass sämmtliche Determinanten $(m+1)^{\text{ter}}$ Ordnung, welche aus dem Systeme

$$w_{i+k} \qquad (i, k = 0, 1, \ldots n-1)$$

gebildet werden können, aber nicht sämmtliche Determinanten m^{ter} Ordnung p als Factor enthalten.

In dieser letzteren Weise sind die Bedingungen für die Existenz von $n-m$ Congruenzwurzeln von Herrn *König* aufgestellt[1]) und von Herrn *Rados* als nothwendig und hinreichend nachgewiesen worden*). Nach der hier eingeführten Terminologie finden die *König*'schen Bedingungen ihren Ausdruck einfach darin,

dass der Rang des Systems

$$w_{i+k} \qquad (i, k = 0, 1, \ldots n-1)$$

in Beziehung auf den Modul p genau gleich m sein soll.

Aber hierfür sind auch schon die je $n-m+1$ Bedingungen $(\mathfrak{S}'.)$ oder $(\mathfrak{S}''.)$ ausreichend, und deren Anzahl ist wesentlich geringer als die Anzahl derjenigen, welche bei der *König*'schen Formulirung gebraucht werden.

Dafür, dass die Congruenz $(\mathfrak{S}.)$ überhaupt eine von Null verschiedene Wurzel habe, genügt die Bedingung:

$$|w_{g+h}| \equiv 0 \pmod{p} \qquad (g, h = 0, 1, \ldots n-1)$$

*) S. 258 dieses Bandes[2]).

[1]) Diese Bedingungen sind von Herrn *Julius König* im Winter 1881/2 in den Uebungen des mathematischen Seminares an der technischen Hochschule zu Budapest mitgetheilt worden. H.

[2]) Vgl. die Anmerkung (1) a. S. 167 dieses Bandes. H.

oder also*):

$$\prod_h \sum_k w_k e^{\frac{2hk\pi i}{n}} \equiv 0 \pmod{p} \qquad (h, k = 0, 1, \ldots n-1),$$

Diese Bedingung findet sich schon — wenn auch unter etwas anderer Form — bei *Schoenemann*. Dass sie in der That genügt, erhellt aus der Congruenz:

$$\prod_h \sum_k w_k e^{\frac{2hk\pi i}{n}} \equiv \prod_h \sum_k w_k g^{hk} \pmod{p} \qquad (h, k = 0, 1, \ldots n-1),$$

in welcher g eine primitive Congruenzwurzel von p bedeutet; diese Congruenz selbst aber ergiebt sich unmittelbar aus der Congruenz:

$$\prod_h (x - e^{\frac{2h\pi i}{n}}) \equiv \prod_h (x - g^h) \pmod{p} \qquad (h = 0, 1, \ldots n-1),$$

wenn man das Lemma benutzt, welches ich im § 1 meiner Inauguraldissertation**) aufgestellt und bewiesen habe.

IV.

Auflösung eines speciellen Systems von Congruenzen.

§ 1.

Die im vorigen Artikel enthaltenen Entwickelungen können zur Auflösung des Systems von n Congruenzen:

$$(1.) \qquad \sum_{k=0}^{k=n-1} w_{h+k} \varphi_k \equiv w_h^0 \pmod{\text{modd. } M', M'', M''', \ldots} \qquad (h = 0, 1, \ldots n-1)$$

*) *Baltzer*'s Determinantenbuch V. Aufl. § 11, 1.

**) Bd. 93 dieses Journals S. 2[1]).

[1]) Band I S. 10—11 dieser Ausgabe von *L. Kronecker*'s Werken. H.

benutzt werden, d. h. sowohl zur Ermittelung der Bedingungen, welchen die als gegeben betrachteten Grössen w und w^0 genügen müssen, damit die Congruenzen Lösungen zulassen, als auch zur Bestimmung der gesuchten n Grössen φ_k selbst im Falle der Lösbarkeit.

Hierbei bedeuten die Grössen M, w, w^0 ganze Grössen eines natürlichen Rationalitätsbereichs $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$. Ueberdies soll — wie im zweiten Theile des § 5 (art. III) — $(M', M'', M''', \ldots)$ ein *Prim*modulsystem und $w_0x^{-1} + w_1x^{-2} + w_2x^{-3} + \cdots$ die Entwickelung des Quotienten der beiden Functionen $\mathfrak{V}(x)$ und $V(x)$, d. i.

$$\mathfrak{v}_0 + \mathfrak{v}_1 x + \cdots + \mathfrak{v}_{n-1}x^{n-1} \quad \text{und} \quad v_0 + v_1 x + \cdots + v_{n-1}x^{n-1} + x^n$$

sein, deren Coefficienten $\mathfrak{v}$ und v ebenfalls als ganze Grössen des Bereichs $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$ vorausgesetzt werden.

Definirt man nun w_n^0, w_{n+1}^0, ... durch die Gleichungen:

$$\sum_{k=0}^{k=n-1} w_{h+k}\varphi_k = w_h^0 \qquad (h = n, n+1, \ldots \text{in inf.}),$$

in welchen die Grössen φ_k eben die den Congruenzen (1.) genügenden Grössen bedeuten, so sind die Grössen w_h^0 durch eine lineare Recursionsformel mit einander verbunden, deren Ordnung höchstens gleich n ist, und die Reihe:

$$\sum_{h=0}^{h=\infty} w_h^0 x^{-h-1}$$

stellt daher eine rationale gebrochene Function von x dar, in welcher der Nenner höchstens vom Grade n ist. Bezeichnet man diese, in reducirter Form, mit $\frac{\mathfrak{W}^0(x)}{V^0(x)}$, so wird das System der Congruenzen (1.) in der Congruenz:

$$\sum_{h=0}^{h=\infty}\sum_{k=0}^{k=n-1} w_{h+k}\varphi_k x^{-h-1} \equiv \frac{\mathfrak{W}^0(x)}{V^0(x)} \quad (\text{modd. } M', M'', \ldots)$$

zusammengefasst, und diese kann, wenn darin für die Reihe:

$$w_0x^{-1} + w_1x^{-2} + w_2x^{-3} + \cdots$$

ihr Werth $\frac{\mathfrak{V}(x)}{V(x)}$ substituirt wird, noch folgendermaassen dargestellt werden:

$$(2.) \qquad \frac{\mathfrak{V}(x)}{V(x)}\sum_{k=0}^{k=n-1}\varphi_k x^k \equiv \frac{\mathfrak{W}^0(x)}{V^0(x)} + G(x) \quad (\text{modd. } M', M'', \ldots),$$

wo $G(x)$ eine ganze Function von x, nämlich:

$$\sum_{k=0}^{k=n-1}\sum_{h=0}^{h=k-1} w_h\varphi_k x^{k-h-1}$$

bedeutet. Multiplicirt man nun diese Congruenz (2.) mit der ganzen Function $\mathfrak{P}(x)$, welche in der letzten der drei Congruenzen ($\overline{\mathfrak{P}}$.) im art. III, § 5 vorkommt, und macht dann von den *beiden* letzten Relationen ($\overline{\mathfrak{P}}$.) Gebrauch, so folgt, dass:

$$(3.) \qquad \frac{E.\sum_{k=0}^{k=n-1}\varphi_k x^k}{Q(x)} \equiv \frac{\mathfrak{V}(x)\mathfrak{W}^0(x)}{V^0(x)} + G_1(x) \quad (\text{modd. } M', M'', \ldots)$$

sein muss, wo $G_1(x)$ eine ganze Function von x bedeutet.

Schon die Congruenz (2.) lehrt, dass der Bruch $\frac{\mathfrak{W}^0(x)}{V^0(x)}$ sich *modulis* M', M'', ... auf einen solchen mit demselben Nenner wie der Bruch $\frac{\mathfrak{V}(x)}{V(x)}$, also nach art. III, § 5, ($\overline{\mathfrak{P}}$.) auf einen Bruch mit dem Nenner $Q(x)$ reduciren lassen muss. *Die hierfür erforderlichen Beziehungen zwischen den Grössen w und w^0 bilden die nothwendigen und hinreichenden Bedingungen für die Lösbarkeit der Congruenzen* (1.).

Wenn die Congruenzen (1.) erfüllt sein sollen, muss sich also die Reihe $w_0^0 x^{-1} + w_1^0 x^{-2} + \cdots$ (im Sinne der Congruenz für das Modulsystem $(M', M'', \ldots)$) durch einen Bruch mit dem Nenner $V(x)$ darstellen lassen. Bei Einführung des Zählers dieses Bruches $V(x) \sum_{h=0}^{h=\infty} w_h^0 x^{-h-1}$ lassen sich aber die Bedingungen der Lösbarkeit der Congruenzen (1.) einfach durch die Congruenz:

$$V(x) \sum_{h=0}^{h=\infty} w_h^0 x^{-h-1} \equiv 0 \quad (\text{modd. } \mathfrak{B}(x),\ V(x),\ M',\ M'', \ldots) \tag{4.}$$

ausdrücken, welche unmittelbar aus der Congruenz (2.) hervorgeht.

Sind die Bedingungen für die Lösbarkeit der Congruenzen (1.) erfüllt, so *bestimmen sich vermöge der Relation* (3.) *die Grössen* φ_k *durch die Congruenz:*

$$E. \sum_{k=0}^{k=n-1} \varphi_k x^k \equiv R(x) + Q(x)S(x) \quad (\text{modd. } M', M'', \ldots), \tag{5.}$$

wenn darin $R(x)$ diejenige ganze Function $(m-1)^{\text{ten}}$ Grades bedeutet, für welche die Differenz:

$$\frac{\mathfrak{B}(x)\mathfrak{B}^0(x)}{V^0(x)} - \frac{R(x)}{Q(x)} \quad (\text{modd. } M', M'', \ldots) \tag{6.}$$

einer ganzen Function von x congruent ist, und wenn ferner für $S(x)$ eine beliebige ganze Function des Grades $n-m-1$ genommen wird. Der Ausdruck auf der rechten Seite der Congruenz (5.) wird alsdann, da $Q(x)$ vom m^{ten} Grade ist, in der That vom Grade $n-1$.

Die in der Congruenz (5.) enthaltene Bestimmung der Grössen φ lässt sich auch im Anschluss an die Bedingungscongruenz (4.) durch die Congruenz:

$$V(x) \sum_{h=0}^{h=\infty} w_h^0 x^{-h-1} \equiv \mathfrak{B}(x) \sum_{k=0}^{k=n-1} \varphi_k x^k \quad (\text{modd. } V(x),\ M',\ M'', \ldots) \tag{7.}$$

ausdrücken, welche sich unmittelbar aus der Congruenz (2.) ergiebt.

Die Function $S(x)$ enthält $n-m$ beliebige Coefficienten; es giebt daher, falls die Congruenzen (1.) überhaupt Lösungen zulassen, eine $(n-m)$-fache Mannigfaltigkeit von Grössen φ_k, welche jenen Congruenzen genügen. Dass dies der Fall ist, wenn die Grössen w_h^0 sämmtlich congruent Null sind, geht schon aus den allgemeinen Entwickelungen im art. II hervor. Die Congruenzen sind dann stets lösbar, und die gesuchten Grössen $\varphi_0, \varphi_1, \ldots \varphi_{n-1}$ bestimmen sich in ihrer $(n-m)$-fachen Mannigfaltigkeit:

> als (dem Integritätsbereich $[\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)}]$ angehörige) Coefficienten irgend einer das Modulsystem $(Q(x), M', M'', \ldots)$ enthaltenden ganzen Function $(n-1)^{\text{ten}}$ Grades von x,

wenn für $Q(x)$ die im art. III, § 1 mit $V^{(m)}(x)$ bezeichnete Determinante:

$$\left| w_{i+k-2}x - w_{i+k-1} \right| \qquad (i, k = 1, 2, \ldots m)$$

genommen wird, und wenn m den Rang des Coefficienten-Systems der Congruenzen (1.) in Beziehung auf das Primmodulsystem $(M', M'', \ldots)$ bedeutet. Denn die im art. III, § 2 hergeleitete Congruenz $W^{(n-m-1)}(x) \equiv 0$ besteht bei den gemachten Annahmen für das Modulsystem $(M', M'', \ldots)$, und die Gleichungen (E.) im art. III, § 1 ergeben dann, dass der Bruch $\frac{\mathfrak{B}(x)}{V(x)}$ sich *modulis* $M', M'', \ldots$ auf den Bruch $\frac{\mathfrak{B}^{(m)}(x)}{V^{(m)}(x)}$ reducirt, dass also in der That die Function $V^{(m)}(x)$ für den oben mit $Q(x)$ bezeichneten Nenner genommen werden kann.

Das hier benutzte Resultat, dass die Rangzahl m mit der Gradzahl der Function $V^{(m)}(x)$ identisch ist, mag an dieser Stelle nochmals hervorgehoben und unabhängig von der vorstehenden Entwickelung folgendermaassen formulirt werden:

> „Sind $w_0, w_1, w_2, \ldots$ ganze Grössen eines natürlichen Rationalitätsbereichs, und wird durch die unendliche Reihe
>
> $$w_0 x^{-1} + w_1 x^{-2} + w_2 x^{-3} + \cdots$$

— im Sinne der Congruenz für ein Primmodulsystem desselben Bereichs — eine rationale Function von x dargestellt, so bezeichnet die Zahl, welche den Rang des Systems:

$$w_{i+k} \qquad (i,\ k = 0,\ 1,\ 2,\ \ldots \text{ in inf.})$$

in Beziehung auf das Modulsystem angiebt, zugleich den niedrigsten Grad, auf welchen der Nenner der durch die Reihe dargestellten Function reducirt werden kann."

Es folgt hieraus, dass auch der *absolute* Rang eines Systems w_{i+k} mit dem Grade des Nenners des durch die Reihe $w_0x^{-1} + w_1x^{-2} + w_2x^{-3} + \cdots$ wirklich dargestellten (reducirten) Bruches übereinstimmt; denn gemäss der Bemerkung am Schlusse des § 5 art. III kann dies als ein *specielleres* Resultat aufgefasst werden.

§ 2.

Für den einfachen Fall des absoluten Rationalitätsbereichs $\mathfrak{R} = 1$ sind $w_0,\ w_1,\ w_2,\ \ldots\ w_0^0,\ w_1^0,\ w_2^0,\ \ldots\ \varphi_0,\ \varphi_1,\ \varphi_2,\ \ldots$ ganze Zahlen, und an die Stelle des Primmodulsystems tritt ein Primmodul p. Nimmt man nun $V(x) = x^n - 1$, so wird für jede ganze Zahl h:

$$w_{h+n} = w_h, \qquad w^0_{h+n} = w^0_h,$$

und es ist demnach:

$$(8.) \qquad \sum_{h=0}^{h=\infty} w_h x^{-h-1} = \frac{\sum_{k=0}^{k=n-1} w_k x^{n-k-1}}{x^n - 1}, \qquad \sum_{h=0}^{h=\infty} w^0_h x^{-h-1} = \frac{\sum_{k=0}^{k=n-1} w^0_k x^{n-k-1}}{x^n - 1}.$$

Für die Lösbarkeit der Congruenzen:

$$(9.) \qquad \sum_{k=0}^{k=n-1} w_{h+k}\varphi_k \equiv w^0_h \pmod{p} \qquad (h = 0,\ 1,\ \ldots\ n-1)$$

ist also — gemäss der Bedingung (4.) im § 1 dieses Artikels — nothwendig und hinreichend, dass die Congruenz:

$$(10.) \qquad \sum_{k=0}^{k=n-1} w^0_k x^{n-k-1} \equiv 0 \pmod{p,\ x^n - 1,\ \sum_{k=0}^{k=n-1} w_k x^{n-k-1}}$$

erfüllt sei, und wenn dies der Fall ist, wird die Bestimmung der Grössen φ gemäss § 1 (7.) durch die Congruenz:

$$(11.) \qquad \sum_{k=0}^{k=n-1} w^0_k x^{n-k-1} \equiv \sum_{k=0}^{k=n-1} \varphi_k x^k \sum_{k=0}^{k=n-1} w_k x^{n-k-1} \pmod{p,\ x^n - 1}$$

gegeben.

Im Falle $n = p - 1$ ist das Modulsystem der Congruenz (10.) dem Systeme $(p,\ (x-x_1)(x-x_2)\ldots)$ aequivalent, wenn $x_1,\ x_2,\ \ldots$ die untereinander und von Null verschiedenen Wurzeln der Congruenz:

$$\sum_{k=0}^{k=p-2} w_k x^{p-k-2} \equiv 0 \pmod{p}$$

bedeuten. Die Congruenzbedingung (10.) besagt demnach nichts Anderes, als dass die Congruenz:

$$\sum_{k=0}^{k=p-2} w^0_k x^{p-k-2} \equiv 0 \pmod{p}$$

für alle von Null verschiedenen Wurzeln der Congruenz:

$$\sum_{k=0}^{k=p-2} w_k x^{p-k-2} \equiv 0 \pmod{p}$$

erfüllt sein muss, und dies ist also nothwendig und hinreichend für die Lösbarkeit der Congruenzen:

$$\sum_{k=0}^{k=p-2} w_{h+k}\varphi_k \equiv w_h^0 \pmod{p} \qquad (h=0, 1, \ldots p-2),$$

in denen $w_{p-1} = w_0$, $w_p = w_1$, $\ldots$ $w_{2p-4} = w_{p-3}$ zu nehmen ist.

Im Falle $n = p$ wird das Modulsystem der Congruenz (10.), da $x^p - 1 \equiv (x-1)^p \pmod{p}$ ist, einem Modulsysteme $(p, (x-1)^{p-m})$ aequivalent, in welchem der Exponent von $x-1$ höchstens $p-1$ sein kann, weil das letzte Element des Modulsystems der Congruenz (10.) nur vom Grade $p-1$ ist*). Die Congruenzbedingung (10.) besagt hiernach, dass

> die Function $\sum_{k=0}^{k=p-1} w_k^0 x^{p-k-1}$ *modulo* p durch die höchste Potenz von $x-1$ theilbar sein muss, welche in der Function $\sum_{k=0}^{k=p-1} w_k x^{p-k-1}$ als Divisor *modulo* p enthalten ist,

und dies ist also nothwendig und hinreichend für die Lösbarkeit der Congruenzen:

$$\sum_{k=0}^{k=p-1} w_{h+k}\varphi_k \equiv w_h^0 \pmod{p} \qquad (h=0, 1, \ldots p-1),$$

in denen $w_p = w_0$, $w_{p+1} = w_1$, $\ldots$ $w_{2p-2} = w_{p-2}$ ist.

Nimmt man alle p Zahlen w^0 gleich *Eins*, so wird:

$$\sum_{k=0}^{k=p-1} w_k^0 x^{p-k-1} \equiv (x-1)^{p-1} \pmod{p},$$

und die Bedingungen der Lösbarkeit der Congruenzen:

$$\sum_{k=0}^{k=p-1} w_{h+k}\varphi_k \equiv 1 \pmod{p} \tag{12.}$$

*) Es wird hierbei natürlich vorausgesetzt, dass nicht alle Grössen w congruent Null sind.

sind daher für jedes beliebige System von Zahlen $w_0, w_1, \ldots w_{p-1}$ erfüllt, falls nur nicht alle durch p theilbar sind. Die allgemeinsten Werthe von $\varphi_0, \varphi_1, \ldots \varphi_{p-1}$ werden hier, gemäss den im § 1 gegebenen Vorschriften, in einfacher Weise durch die Congruenz:

$$\sum_{k=0}^{k=p-1} \varphi_k x^k \equiv r(x-1)^{m-1} \pmod{p, (x-1)^m} \tag{13.}$$

definirt, und die Zahlen m und r sind dabei durch die Congruenzen:

$$\sum_{k=0}^{k=p-1} w_k x^{p-k-1} \equiv (x-1)^{p-m}\psi(x), \quad r\psi(1) \equiv 1 \pmod{p} \tag{14.}$$

bestimmt, welche $(x-1)^{p-m}$ als die höchste in $\sum_{k=0}^{k=p-1} w_k x^{p-k-1}$ (*modulo* p) enthaltene Potenz von $x-1$ charakterisiren.

Dass die so definirten Grössen φ in der That den Congruenzen (12.) genügen, zeigt sich unmittelbar, wenn man die beiden Congruenzen (13.) und (14.) mit einander multiplicirt. Dann kommt nämlich:

$$\sum_{k=0}^{k=p-1} w_k x^{p-k-1} \sum_{k=0}^{k=p-1} \varphi_k x^k \equiv r\psi(x)(x-1)^{p-1} \pmod{p, (x-1)^p},$$

und da:

$$r\psi(x) \equiv 1 \pmod{p, x-1}, \quad (x-1)^{p-1} \equiv 1 + x + x^2 + \cdots + x^{p-1} \pmod{p},$$

$$\sum_k w_k x^{p-k-1} \sum_k \varphi_k x^k \equiv \sum_{h,k} w_{h+k}\varphi_k x^{p-h-1} \pmod{x^p - 1} \quad (h, k=0, 1, \ldots p-1)$$

ist, so resultirt die Congruenz:

$$\sum_{h,k} w_{h+k}\varphi_k x^{p-h-1} \equiv \sum_h x^{p-h-1} \pmod{p, x^p - 1} \quad (h, k=0, 1, \ldots p-1),$$

aus welcher die p Congruenzen (12.) offenbar folgen.

Die Lösbarkeit der Congruenzen (12.) brauchte ich als Lemma für Sätze aus der Theorie der algebraischen Gleichungen, welche ich in meinen öffentlichen Universitätsvorlesungen in diesem Wintersemester entwickelt habe. Ich habe dabei zwei verschiedene, jedoch etwas complicirte Beweise für das Lemma gegeben. Aber Herr *Runge*, welcher den Vorlesungen beiwohnte, hat dann einen einfacheren Beweis gefunden, und mir eine Mittheilung darüber gemacht, welche mich auf die obige Beweismethode und auch auf die Behandlung des allgemeineren Problems in § 1 dieses Artikels geführt hat.

§ 3.

Nimmt man für die Grössen w_k^0 in den Congruenzen (1.) des § 1 dieses Artikels die Grössen w_{k+n}, so wird diesen Congruenzen offenbar durch die Werthe:

$$\varphi_k \equiv -v_k \pmod{M', M'', \ldots} \qquad (k=0, 1, \ldots n-1)$$

genügt, da die Grössen v und w durch die Relationen:

$$w_{k+n} + \sum_{k=0}^{k=n-1} v_k w_{k+k} = 0 \qquad (k=0, 1, 2, \ldots) \tag{15.}$$

mit einander verbunden sind. Es sind dies aber nur dann die *einzigen* genügenden Werthe der Grössen φ_k, wenn der Rang des Systems:

$$w_{i+k} \qquad (i, k=0, 1, 2, \ldots \text{in inf.})$$

in Beziehung auf das Modulsystem $(M', M'', \ldots)$ genau gleich n ist. Für die hier angenommenen Werthe der Grössen w_k^0 wird nämlich:

$$\frac{\mathfrak{B}^0(x)}{V^0(x)} = \frac{\mathfrak{B}(x)}{V(x)} x^n - \sum_{k=0}^{k=n-1} w_k x^{n-k-1},$$

und wenn man hierin x^n durch $V(x) - \sum_{k=0}^{k=n-1} v_k x^k$ ersetzt, so bestimmt sich

vermöge der Congruenz (5.) des § 1 die Function $\sum_{k=0}^{k=n-1} \varphi_k x^k$ als der Rest der Division von:

$$-\sum_{k=0}^{k=n-1} v_k x^k$$

durch $Q(x)$, unter Hinzufügung eines Ausdrucks $Q(x)S(x)$, in welchem $S(x)$ eine beliebige ganze Function des Grades $n-m-1$ bedeutet. Nur dann also, wenn die Zahl m, welche den Rang des Systems w_{i+k} bezeichnet, genau gleich n ist, werden die Grössen φ_k durch die Congruenz:

$$\sum_{k=0}^{k=n-1} \varphi_k x^k \equiv -\sum_{k=0}^{k=n-1} v_k x^k \pmod{M', M'', \ldots}$$

vollständig bestimmt.

Nach den im § 1 gemachten Voraussetzungen ist $V(x)$ eine ganze Grösse des Bereichs $(x, \mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$. Ist nun diese Grösse $V(x)$ irreductibel, so kann sie keinen Factor niedrigeren Grades $Q(x)$ haben, und zwar auch nicht im Sinne der Congruenz für das Modulsystem $(M', M'', \ldots)$, wenn die Irreductibilität von $V(x)$ in demselben Sinne vorausgesetzt wird. Der Rang des Systems w_{i+k} in Beziehung auf das Modulsystem $(M', M'', \ldots)$ kann dann also niemals kleiner als n sein, welche Grössen des Bereichs $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$ man auch für die Grössen v nehmen mag. An Stelle der Grössen v kann man aber auch, wie schon im art. III, § 3 [S. 180] erwähnt worden, die ersten n Grössen w beliebig annehmen.

Die Irreductibilität einer ganzen Function von x:

$$v_0 + v_1 x + v_2 x^2 + \cdots + v_{n-1} x^{n-1} + x^n,$$

in Beziehung auf ein Modulsystem $(M', M'', \ldots)$, lässt sich hiernach dadurch charakterisiren, dass der Rang des Systems:

w_{i+k} $(i, k = 0, 1, \ldots n-1)$

stets gleich n ist, wenn für $w_0, w_1, \ldots w_{n-1}$ beliebige ganze Grössen desselben Bereichs $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$ genommen werden, dem die Coefficienten $v_0, v_1, \ldots v_{n-1}$ angehören, und wenn ferner die Grössen $w_n, w_{n+1}, \ldots w_{2n-2}$ mittels der Relationen (15.) aus den ersten n Grössen w und den Grössen v bestimmt werden.

EIN FUNDAMENTALSATZ DER ALLGEMEINEN ARITHMETIK.

VON

L. KRONECKER.

Crelle, Journal für die reine und angewandte Mathematik. Band 100. S. 490—510.

EIN FUNDAMENTALSATZ DER ALLGEMEINEN ARITHMETIK.

Die arithmetische Behandlung der algebraischen Grössen führt mit Nothwendigkeit dazu, den *Gauss*'schen Congruenzbegriff so zu erweitern, dass auch „Systeme von Moduln“ an Stelle des einfachen Congruenzmoduls zugelassen werden. Bei der weiteren Ausbildung der Theorie der Modulsysteme zeigt sich aber, dass dadurch zugleich die Untersuchung der algebraischen Grössen auf die der rationalen Functionen von Variabeln reducirt wird*). Es lag daher die Vermuthung nahe, dass die Theorie der Modulsysteme das Mittel gewähren möchte, bei der arithmetischen Behandlung der algebraischen Grössen die Auffassung derselben als „irrationaler Grössen“ überhaupt entbehrlich zu machen und in den bezüglichen Gebieten der Algebra in principieller Weise die algebraischen Grössen durch rationale zu ersetzen. Dass dies in der That der Fall ist, soll in den folgenden Entwickelungen gezeigt werden, deren Zielpunkt

> *die Bestimmung eines Primmodulsystems ist, für welches eine gegebene ganze Function einer Variabeln sich als Product von Linearfactoren darstellen lässt.*

Die vorliegende Abhandlung enthält somit eine „Anwendung der Modulsysteme auf eine elementare algebraische Frage“, und sie kann demgemäss

*) Vgl. die Einleitung in meiner Festschrift zu Herrn *Kummer*'s Doctorjubiläum, Bd. 92 dieses Journals S. 2[1]).

[1]) Band II S. 246—247 dieser Ausgabe von *L. Kronecker*'s Werken. H.

als eine Fortsetzung meines im 99. Bande dieses Journals[1]) veröffentlichten Aufsatzes angesehen werden, an welchen sie sich auch in den Definitionen und Bezeichnungen aufs Genaueste anschliesst.

Da die Theorie der Modulsysteme den Begriff der algebraischen Grössen, in dem bisherigen Sinne, bei arithmetischen Untersuchungen überflüssig erscheinen lässt, so genügt es, die Arithmetik auf die Behandlung *ganzer ganzzahliger Functionen unbestimmter Variabeln* auszudehnen. Die arithmetische Theorie solcher Functionen, d. h. also:

> *die arithmetische Theorie ganzer Grössen eines beliebigen natürlichen Rationalitätsbereichs*

ist es, die ich mit dem im Titel vorkommenden Ausdruck: *„allgemeine Arithmetik"* in passender Weise zu bezeichnen glaube. Dass für das hiermit charakterisirte mathematische Gebiet die *Zerlegung der ganzen Functionen einer Variabeln in lineare Factoren im Sinne der Congruenz für ein Primmodulsystem* von fundamentaler Bedeutung ist, bedarf keiner näheren Darlegung; es genügt vielmehr der Hinweis darauf, dass auch jener Satz über die Zerlegung im gewöhnlichen Sinne in der Regel, nach dem Vorgange von *Gauss*, als ein Fundamentalsatz der Algebra aufgefasst und bezeichnet wird.

Die Wichtigkeit der Bestimmung eines *Prim*modulsystems besteht darin, dass nur Congruenzen für *Prim*modulsysteme genau wie Gleichungen behandelt werden können, weil nur für Primmodulsysteme aus der Congruenz $A \cdot B \equiv 0$ geschlossen werden kann, dass entweder A oder B congruent Null sein muss.

§ 1.

Bedeuten $c_1, c_2, \ldots c_n$ *ganze* Grössen des natürlichen Rationalitätsbereichs $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$, und setzt man:

$$F(x) = x^n - c_1 x^{n-1} + c_2 x^{n-2} - \cdots \pm c_n,$$

[1]) Ueber einige Anwendungen der Modulsysteme auf elementare algebraische Fragen. Bd. III S. 147—208 dieser Ausgabe von *L. Kronecker's* Werken. H.

so ist $F(x)$ eine ganze Grösse des Bereichs $(x, \mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$. Bezeichnet man nun ferner, wie im § 11 meiner mehrerwähnten Festschrift, mit $\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n$ die n durch die Gleichung:

$$(x - x_1)(x - x_2) \cdots (x - x_n) = x^n - \mathfrak{f}_1 x^{n-1} + \mathfrak{f}_2 x^{n-2} - \cdots \pm \mathfrak{f}_n$$

definirten elementaren symmetrischen Functionen der unbestimmten Variabeln $x_1, x_2, \ldots x_n$, so besteht die Congruenz:

$$(1.) \qquad F(x) \equiv (x - x_1)(x - x_2) \cdots (x - x_n) \pmod{\mathfrak{f}_1 - c_1,\ \mathfrak{f}_2 - c_2, \ldots \mathfrak{f}_n - c_n}$$

oder, wenn zur Abkürzung:

$$(x - x_1)(x - x_2) \cdots (x - x_n) = \mathfrak{F}(x)$$

gesetzt wird:

$$(1^*.) \qquad F(x) \equiv \mathfrak{F}(x) \pmod{\mathfrak{f}_1 - c_1,\ \mathfrak{f}_2 - c_2, \ldots \mathfrak{f}_n - c_n}.$$

Das Modulsystem dieser Congruenz, welches offenbar vom Range n ist, kann aber andere Modulsysteme n^{ter} Stufe enthalten, und es handelt sich also darum, für jedes gegebene System von Coefficienten c ein *Prim*modulsystem n^{ter} Stufe zu bestimmen, für welches die Elemente jenes Modulsystems: $\mathfrak{f}_1 - c_1, \mathfrak{f}_2 - c_2, \ldots \mathfrak{f}_n - c_n$ sämmtlich congruent Null werden. Dabei kann $F(x)$ offenbar als eine solche Grösse des Bereichs $(x, \mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$ vorausgesetzt werden, die als Product von lauter von einander verschiedenen irreductibeln Factoren darstellbar ist und daher mit der nach x genommenen Ableitung von $F(x)$ keinen Factor gemein hat.

§ 2.

Setzt man, ähnlich wie im § 11 meiner oben citirten Festschrift:

$$G(z, \mathfrak{f}_1, \mathfrak{f}_2, \dots \mathfrak{f}_n) = \prod_{(i)} (z - u_1 x_{i_1} - u_2 x_{i_2} - \cdots - u_n x_{i_n}),$$

wo das Product über alle $n!$ Permutationen $(i_1, i_2, \dots i_n)$ zu erstrecken ist, so wird G eine ganze ganzzahlige Function von $z, \mathfrak{f}_1, \mathfrak{f}_2, \dots \mathfrak{f}_n, u_1, u_2, \dots u_n$. Unter den Grössen u werden „*Unbestimmte*“ verstanden, und gemäss der a. a. O. adoptirten Bezeichnung ist $G(z, \mathfrak{f}_1, \mathfrak{f}_2, \dots \mathfrak{f}_n) = 0$ eine zur Gleichung $\mathfrak{F}(x) = 0$ „gehörige“ oder von derselben „abgeleitete *Galois*'sche Gleichung“. Es kann daher auch füglich $G(z, \mathfrak{f}_1, \mathfrak{f}_2, \dots \mathfrak{f}_n)$ selbst eine „*von der Function* $\mathfrak{F}(x)$ *abgeleitete Galois'sche Function*“ genannt werden.

Nach der im § 12 meiner Festschrift entwickelten Theorie der „Gattungen von Functionen“ gehört $u_1 x_1 + u_2 x_2 + \cdots + u_n x_n$ zur *Galois*'schen Gattung von Functionen von $x_1, x_2, \dots x_n$. Jede der Grössen x selbst gehört daher zum Gattungs*bereich* von $u_1 x_1 + u_2 x_2 + \cdots + u_n x_n$, und es besteht also für jeden Werth $k = 1, 2, \dots n$ eine identische Gleichung:

$$(2.) \quad \left\{ \begin{array}{c} x_k \psi(\mathfrak{f}_1, \mathfrak{f}_2, \dots \mathfrak{f}_n;\ u_1, u_2, \dots u_n) \\ = \varphi_k(u_1 x_1 + u_2 x_2 + \cdots + u_n x_n;\ \mathfrak{f}_1, \mathfrak{f}_2, \dots \mathfrak{f}_n;\ u_1, u_2, \dots u_n), \end{array} \right.$$

in welcher ψ und φ_k ganze ganzzahlige Functionen der in den Parenthesen vorkommenden Grössen bedeuten. Die Function ψ ist nichts Anderes als die Discriminante der *Galois*'schen Function $G(z)$; sie ist daher nach dem, was ich am Schlusse des citirten § 12 meiner Festschrift nachgewiesen habe, *das Product einer primitiven Form der Unbestimmten u und einer Potenz der Discriminante von* $\mathfrak{F}(x)$. Da nun die Function $F(x)$ als Product von lauter *verschiedenen* irreductibeln Factoren vorausgesetzt worden, so ist ihre Discriminante von Null verschieden, und es ist demnach auch:

$$\psi(c_1, c_2, \dots c_n;\ u_1, u_2, \dots u_n) \gtrless 0.$$

Die Congruenz:

$$(2^*.) \quad \left\{ \begin{array}{c} x_k \psi(c_1, c_2, \dots c_n;\ u_1, u_2, \dots u_n) \\ \equiv \varphi_k(u_1 x_1 + u_2 x_2 + \cdots + u_n x_n;\ c_1, c_2, \dots c_n;\ u_1, u_2, \dots u_n) \\ (\text{modd. } \mathfrak{f}_1 - c_1,\ \mathfrak{f}_2 - c_2, \dots \mathfrak{f}_n - c_n), \end{array} \right.$$

welche unmittelbar aus der mit (2.) bezeichneten Gleichung folgt, wird demgemäss für irreductible Functionen $F(x)$ niemals illusorisch.

Die Gleichung (2.) kann durch die Congruenz:

$$(2^{**}.) \quad x_k \psi(\dots \mathfrak{f}_h, \dots) \equiv \varphi_k(z; \dots \mathfrak{f}_h, \dots) \pmod{z - u_1 x_1 - u_2 x_2 - \cdots - u_n x_n}_{(h=1, 2, \dots n)}$$

ersetzt werden, in welcher — der Einfachheit halber — die Unbestimmten u unter den Functionszeichen ψ und φ_k weggelassen worden sind. Substituirt man die hieraus resultirenden Congruenzwerthe von $x_1, x_2, \dots x_n$ in dem Product $(x - x_1)(x - x_2) \dots (x - x_n)$, so kommt:

$$\psi(\dots \mathfrak{f}_h, \dots)^n \mathfrak{F}(x) \equiv \prod_k (x\psi(\dots \mathfrak{f}_h, \dots) - \varphi_k(z; \dots \mathfrak{f}_h, \dots)) \qquad (h, k = 1, 2, \dots n),$$

und diese Congruenz muss, da sie nur *symmetrische* Functionen von $x_1, x_2, \dots x_n$ enthält, nicht bloss für den Modul $z - u_1 x_1 - u_2 x_2 - \cdots - u_n x_n$, sondern für jeden der $n!$ Moduln:

$$z - u_1 x_{i_1} - u_2 x_{i_2} - \cdots - u_n x_{i_n},$$

also auch für deren Product, d. h. für den Modul $G(z, \mathfrak{f}_1, \mathfrak{f}_2, \dots \mathfrak{f}_n)$ gelten. Hiernach besteht die Congruenz:

$$(3.) \quad \psi(\dots \mathfrak{f}_h, \dots)^n \mathfrak{F}(x) \equiv \prod_k (x\psi(\dots \mathfrak{f}_h, \dots) - \varphi_k(z; \dots \mathfrak{f}_h, \dots)) \pmod{G(z; \dots \mathfrak{f}_h \dots)}$$
$$(h, k = 1, 2, \dots n),$$

und wenn man darin $\mathfrak{f}_1 = c_1$, $\mathfrak{f}_2 = c_2$, ... $\mathfrak{f}_n = c_n$ setzt, so wird:

$$(3^*.) \qquad \psi(\ldots c_h, \ldots)^n F(x) \equiv \prod_{h,\,k=1,\,2,\,\ldots\,n} (x\psi(\ldots c_h, \ldots) - \varphi_k(z; \ldots c_h, \ldots)) \pmod{G(z; \ldots c_h, \ldots)}$$

Diese letztere Congruenz zeigt, dass jede ganze Function von x sich im Sinne einer Congruenz als Product von Linearfactoren darstellen lässt, wenn man die zugehörige *Galois*'sche Function als Modul nimmt. Denkt man sich nun $G(z; \ldots c_h, \ldots)$ als ganze Grösse des Bereichs $(z, \mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$ in irreductible Factoren zerlegt und bezeichnet irgend einen dieser irreductibeln Factoren mit $G_1(z)$, so ist:

$$(3^{**}.) \qquad \psi(\ldots c_h, \ldots)^n F(x) \equiv \prod_{h,\,k=1,\,2,\,\ldots\,n} (x\psi(\ldots c_h, \ldots) - \varphi_k(z; \ldots c_h, \ldots)) \pmod{G_1(z)}$$

und diese Congruenz enthält die Darstellung von $F(x)$ als Product von Linearfactoren für einen *Primmodul;* eine Darstellung, durch welche man der Einführung „algebraischer Grössen" bei vielen, nachher näher zu präcisirenden, algebraischen Untersuchungen enthoben wird.

An Stelle der Unbestimmten u, welche in den Functionen φ, ψ, G vorkommen, können auch beliebige ganze Zahlen genommen werden; nur müssen sie so gewählt werden, dass ψ von Null verschieden ist. So kann man z. B. für:

$$F(x) = x^3 - c_3$$

$u_1 = 0$, $u_2 = 1$, $u_3 = -1$ nehmen. Alsdann wird $G(z; \ldots c_h, \ldots) = z^6 + 27c_3^3$, und wenn nun c_3 nicht die dritte Potenz einer ganzen Grösse des Rationalitätsbereichs $(\mathfrak{R}', \mathfrak{R}'', \ldots)$ ist, so ist $z^6 + 27c_3^3$ irreductibel, und dieser Ausdruck selbst ist also an Stelle von $G_1(z)$ als Primmodul zu brauchen. Die Congruenz (3**.) geht in diesem Falle in folgende über:

$$(3^0.) \qquad 4\cdot(9c_3)^3(x^3 - c_3) \equiv (9c_3x - z^4)(18c_3x + 9c_3z + z^4)(18c_3x - 9c_3z + z^4) \pmod{z^6 + 27c_3^3},$$

und diese wird, wenn man darin $c_3 = 2$ setzt, mit derjenigen übereinstimmend, welche ich im Anfange des Jahres 1885 Herrn *P. Mansion* brieflich mitgetheilt habe, und welche alsdann in der *Mathesis* vom Mai 1885 abgedruckt worden ist[1]). — Ist $c_3 = a^3$ und a eine Grösse des Rationalitätsbereichs $(\mathfrak{R}', \mathfrak{R}'', \ldots)$, so ist $z^2 + 3a^2$ einer der irreductibeln Factoren von $z^6 + 27c_3^3$, und es kommt:

$$4(x^3 - a^3) \equiv (x - a)(2x + z + a)(2x - z + a) \pmod{z^2 + 3a^2},$$

wodurch die Einführung von $\sqrt{-3}$ bei der Factorenzerlegung von $x^3 - a^3$ vermieden wird.

§ 3.

Für das Modulsystem, dessen n Elemente sind:

$$x_k\psi(\ldots c_h, \ldots) - \varphi_k(z; \ldots c_h, \ldots) \qquad (h,\,k=1,\,2,\,\ldots\,n)$$

ist offenbar:

$$\psi(\ldots c_h, \ldots)^n \mathfrak{F}(x) \equiv \prod_k (x\psi(\ldots c_h, \ldots) - \varphi_k(z; \ldots c_h, \ldots)) \qquad (h,\,k=1,\,2,\,\ldots\,n).$$

Verbindet man diese Congruenz mit der Congruenz (3**.) des § 2, so ergiebt sich, dass die Congruenz:

$$(4.) \qquad \psi(\ldots c_h, \ldots)^n \mathfrak{F}(x) \equiv \psi(\ldots c_h, \ldots)^n F(x)$$

für das Modulsystem:

$$(\mathfrak{R}) \qquad (G_1(z); \ldots, x_k\psi(\ldots c_h, \ldots) - \varphi_k(z; \ldots c_h, \ldots), \ldots) \qquad (h,\,k=1,\,2,\,\ldots\,n)$$

[1]) *P. Mansion*, Une équivalence algébrique; Mathesis, mai 1885, t. V. p. 102. H.

bestehen muss. Die Elemente dieses Modulsystems sind ganze Grössen des natürlichen Rationalitätsbereichs:

$$(z, x_1, x_2, \ldots x_n, \mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)}),$$

also ganze ganzzahlige Functionen dieser $n+n$ unbestimmten Variabeln. Es ist ein *Prim*modulsystem, weil $G_1(z)$ irreductibel und jedes der andern Elemente in den Grössen x linear ist; es ist ferner offenbar vom Range $n+1$.

Da das mit $(\mathfrak{M})$ bezeichnete Modulsystem *prim* ist, so kann in der Congruenz (4.) der Factor ψ^n, welcher offenbar das Modulsystem nicht enthält, weggelassen werden, und es ist also:

$$\mathfrak{F}(x) \equiv F(x) \pmod{(\mathfrak{M})}, \tag{4*.}$$

oder, wenn auf beiden Seiten der Congruenz nach Potenzen von x entwickelt wird:

$$\mathfrak{f}_h \equiv c_h \pmod{(\mathfrak{M})} \qquad (h=1, 2, \ldots n). \tag{4**.}$$

Bezeichnet man nun, wie im § 12 (S. 38) meiner mehrfach citirten Festschrift[1]), mit $\mathfrak{g}(x_1, x_2, \ldots x_n)$ eine ganze Function einer Gattung ϱ^{ter} Ordnung und mit $\Phi(\mathfrak{g}, \mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n) = 0$ die Gleichung ϱ^{ten} Grades, welcher die Function $\mathfrak{g}$ genügt, so ist:

$$\prod_{(\varphi)}(y - \mathfrak{g}(x_{\varrho_1}, x_{\varrho_2}, \ldots x_{\varrho_n})) = \Phi(y, \mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n),$$

wo sich die Multiplication auf alle diejenigen Permutationen $(\varrho_1, \varrho_2, \ldots \varrho_n)$ erstreckt, für welche die Function $\mathfrak{g}$ verschiedene (conjugirte) Werthe annimmt. Es besteht also die Congruenz:

$$\prod_{(\varphi)}(y - \mathfrak{g}(x_{\varrho_1}, x_{\varrho_2}, \ldots x_{\varrho_n})) \equiv \Phi(y, c_1, c_2, \ldots c_n)$$

[1]) Band II S. 289 dieser Ausgabe. H.

für das Modulsystem $(\mathfrak{f}_1 - c_1, \mathfrak{f}_2 - c_2, \ldots \mathfrak{f}_n - c_n)$ und also auch für das Modulsystem $(\mathfrak{M})$, da dieses, gemäss der Congruenz (4**.), in dem ersteren enthalten ist. Wenn nun die Gleichung $\Phi(y, c_1, c_2, \ldots c_n) = 0$ durch einen Werth $y = c$ befriedigt wird, der dem Rationalitätsbereich $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$ angehört und demnach auch eine *ganze* Grösse dieses Bereichs sein muss, so wird:

$$\prod_{(\varphi)}(c - \mathfrak{g}(x_{\varrho_1}, x_{\varrho_2}, \ldots x_{\varrho_n})) \equiv 0 \pmod{(\mathfrak{M})}.$$

Weil aber das Modulsystem $(\mathfrak{M})$ prim ist, muss mindestens einer der Factoren dieses Products congruent Null sein, und man kann daher annehmen, dass:

$$\mathfrak{g}(x_1, x_2, \ldots x_n) \equiv c \pmod{(\mathfrak{M})} \tag{5.}$$

ist, da man ja, falls die conjugirte Function $\mathfrak{g}(x_{\varrho_1}, x_{\varrho_2}, \ldots x_{\varrho_n})$ congruent c wäre, diese selbst als $\mathfrak{g}'(x_1, x_2, \ldots x_n)$ bezeichnen und als die erste der conjugirten Functionen nehmen könnte.

Es sei nun $\mathfrak{g}_0$ eine ganze Function einer Gattung *höchster* Ordnung, für welche die entsprechende Gleichung $\Phi_0(y) = 0$ eine rationale Wurzel und dabei eine von Null verschiedene Discriminante hat. Es seien ferner $\mathfrak{g}_0', \mathfrak{g}_0'', \mathfrak{g}_0''', \ldots$ Functionen des durch $\mathfrak{g}_0$ repräsentirten Gattungsbereichs, und zwar seien $\mathfrak{g}_0', \mathfrak{g}_0'', \mathfrak{g}_0''', \ldots$ ganze ganzzahlige Functionen von $x_1, x_2, \ldots x_n$, welche ausreichend sind, um *jede* ganze ganzzahlige Function des Gattungsbereichs $(\mathfrak{g}_0)$ als *lineare* homogene Function von $\mathfrak{g}_0', \mathfrak{g}_0'', \mathfrak{g}_0''', \ldots$ so darzustellen, dass die Coefficienten ganze ganzzahlige Functionen von $\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n$ werden. Die Functionen $\mathfrak{g}_0', \mathfrak{g}_0'', \mathfrak{g}_0''', \ldots$ bilden dann die Elemente eines Fundamentalsystems der Gattung $\mathfrak{g}_0$, und für alle diese Functionen $\mathfrak{g}_0$ bestehen Congruenzen:

$$\mathfrak{g}_0' \equiv c_0', \quad \mathfrak{g}_0'' \equiv c_0'', \quad \mathfrak{g}_0''' \equiv c_0''', \ldots \pmod{(\mathfrak{M})},$$

in welchen $c_0', c_0'', c_0''', \ldots$ ganze Grössen des Bereichs $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$ bedeuten. Denn gemäss den Entwickelungen über die Theorie der Gattungen

im § 12 meiner Festschrift existirt für jede dieser Functionen $\mathfrak{g}_0', \mathfrak{g}_0'', \mathfrak{g}_0''', \ldots$ eine Gleichung:

$$(6.) \qquad \mathfrak{g}_0^{(h)}(x_1, x_2, \ldots x_n)\,\overline{\psi}(\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n) = \overline{\varphi}_h(\mathfrak{g}_0(x_1, x_2, \ldots x_n), \mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n),$$

in welcher $\overline{\varphi}_h$ und $\overline{\psi}$ ganze ganzzahlige Functionen der in den Parenthesen enthaltenen Grössen bedeuten. Dabei ist $\overline{\psi}$ nichts Anderes als die Discriminante jener Gleichung $\Phi_0(y, \mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n) = 0$, welcher $\mathfrak{g}_0(x_1, x_2, \ldots x_n)$ genügt, und es ist daher der Voraussetzung nach $\overline{\psi}(c_1, c_2, \ldots c_n) \gtrless 0$. Aus der Gleichung (6.) folgt aber die Congruenz:

$$(7.) \qquad \mathfrak{g}_0^{(h)}(x_1, x_2, \ldots x_n)\,\overline{\psi}(c_1, c_2, \ldots c_n) \equiv \overline{\varphi}_h(\mathfrak{g}_0(x_1, x_2, \ldots x_n), c_1, c_2, \ldots c_n) \pmod{(\mathfrak{M})},$$

da, wie oben gezeigt worden, $\mathfrak{f}_h \equiv c_h \pmod{(\mathfrak{M})}$ für jeden Index h ist, und hieraus ergiebt sich mit Hülfe der Congruenz (5.), dass in der That:

$$(5^*.) \qquad \mathfrak{g}_0^{(h)}(x_1, x_2, \ldots x_n) \equiv c_0^{(h)} \pmod{(\mathfrak{M})}$$

wird, wenn man $c_0^{(h)}$ mittels der Congruenz:

$$c_0^{(h)}\,\overline{\psi}(c_1, c_2, \ldots c_n) \equiv \overline{\varphi}_h(c_0, c_1, c_2, \ldots c_n) \pmod{(\mathfrak{M})}$$

bestimmt.

§ 4.

Die im zweiten Paragraphen gebrauchte Zerlegung der *Galois*'schen Function $G(z, c_1, c_2, \ldots c_n)$ in ihre irreductibeln Factoren führt auch zur Bestimmung der am Schlusse des § 3 charakterisirten, durch $\mathfrak{g}', \mathfrak{g}'', \mathfrak{g}''', \ldots$ repräsentirten Gattung von Functionen. Bedeuten nämlich $u_1^0, u_2^0, \ldots u_n^0$ „unbestimmte" Grössen und setzt man analog den obigen Bezeichnungen:

$$\prod_{(i)}(z^0 - u_1^0 x_{i_1} - u_2^0 x_{i_2} - \cdots - u_n^0 x_{i_n}) = G^0(z^0, \mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n),$$

so wird vermöge der mit (4**.) bezeichneten Congruenzen:

$$\prod_{(i)}(z^0 - u_1^0 x_{i_1} - u_2^0 x_{i_2} - \cdots - u_n^0 x_{i_n}) \equiv G^0(z^0, c_1, c_2, \ldots c_n) \pmod{(\mathfrak{M})}.$$

Die Multiplication ist hier über alle Permutationen $(i_1, i_2, \ldots i_n)$ zu erstrecken. Denkt man sich nun $G^0(z^0, c_1, c_2, \ldots c_n)$ in irreductible Factoren zerlegt, so muss, da $(\mathfrak{M})$ ein *Prim*modulsystem ist, für jeden bestimmten Werth $z^0 = u_1^0 x_{i_1} + u_2^0 x_{i_2} + \cdots + u_n^0 x_{i_n}$ mindestens *einer* dieser irreductibeln Factoren mod. $(\mathfrak{M})$ congruent Null werden. Da aber eine Congruenz $f(z) \equiv 0$ für ein *Prim*modulsystem nicht mehr Congruenzwurzeln haben kann, als der Grad der ganzen Function $f(z)$ beträgt, so muss *jeder* irreductible Factor von $G^0(z^0, c_1, c_2, \ldots c_n)$ für so viel Werthe $z^0 = u_1^0 x_{i_1} + u_2^0 x_{i_2} + \cdots + u_n^0 x_{i_n}$ congruent Null werden, als sein Grad in Beziehung auf z^0 beträgt. Es muss daher, wenn $G_1^0(z^0)$ derjenige irreductible Factor von $G^0(z^0, c_1, c_2, \ldots c_n)$ ist, welcher für $z^0 = u_1^0 x_1 + u_2^0 x_2 + \cdots + u_n^0 x_n$ congruent Null wird, eine Congruenz bestehen:

$$(8.) \qquad G_1^0(z^0) \equiv \prod_{(r)}(z^0 - u_1^0 x_{r_1} - u_2^0 x_{r_2} - \cdots - u_n^0 x_{r_n}) \pmod{(\mathfrak{M})},$$

wo sich die Multiplication auf gewisse Permutationen $(r_1, r_2, \ldots r_n)$ bezieht, zu denen die Permutation $(1, 2, \ldots n)$ gehört, und deren Anzahl gleich dem Grade von $G_1^0(z^0)$ ist.

Wenn man in der Congruenz (2*.) des § 2 die Unbestimmten u^0 für die Unbestimmten u substituirt, ferner die Grössen $x_1, x_2, \ldots x_n$ in $x_{r_1}, x_{r_2}, \ldots x_{r_n}$ permutirt und endlich das Modulsystem $(\mathfrak{f}_1 - c_1, \mathfrak{f}_2 - c_2, \ldots \mathfrak{f}_n - c_n)$ durch das gemäss den Congruenzen (4**.) darin enthaltene, mit $(\mathfrak{N})$ bezeichnete Modulsystem ersetzt, so resultirt die Congruenz:

$$(9.) \qquad \begin{cases} x_{r_h}\,\psi(c_1, c_2, \ldots c_n;\ u_1^0, u_2^0, \ldots u_n^0) \\ \equiv \varphi_h(u_1^0 x_{r_1} + u_2^0 x_{r_2} + \cdots + u_n^0 x_{r_n};\ c_1, c_2, \ldots c_n;\ u_1^0, u_2^0, \ldots u_n^0) \pmod{(\mathfrak{M})}, \end{cases}$$

welche zeigt, dass jede der Grössen x sich mod. $(\mathfrak{M})$ als rationale Function irgend einer der Wurzeln der Congruenz $G_1^0(z^0) \equiv 0 \pmod{(\mathfrak{M})}$ darstellen lässt. Jede dieser Congruenzwurzeln selbst ist also mod. $(\mathfrak{M})$ eine rationale Function jeder andern, und wenn man diese Congruenzwurzeln mit $z_1^0, z_2^0, \ldots z_r^0$ bezeichnet, so ist daher:

$$(10.) \qquad z_h^0 \equiv \theta_h^{(k)}(z_k^0), \quad G_1^0(z^0) \equiv \prod_h (z^0 - z_k^0) \pmod{(\mathfrak{M})} \qquad (h, k = 1, 2, \ldots r),$$

wo $\theta_h^{(k)}(z^0)$ eine ganze Function von z^0 bedeutet, deren Coefficienten rationale Functionen der unbestimmten Variabeln $\mathfrak{R}$ und der Unbestimmten u^0 sind. Aus den Congruenzen (10.) erhellt, dass die Functionen $\theta_h^{(k)}$, mod. $(\mathfrak{M})$ betrachtet, eine *Gruppe* bilden. Denn das Product:

$$\left(z^0 - \theta_h^{(k)}(z_1^0)\right)\left(z^0 - \theta_h^{(k)}(z_2^0)\right) \cdots \left(z^0 - \theta_h^{(k)}(z_r^0)\right),$$

welches offenbar den Factor $z^0 - z_h^0$ enthält, ist mod. $(\mathfrak{M})$ einer ganzen Function von z^0 congruent, deren Coefficienten rationale Functionen der Grössen $\mathfrak{R}$ und u^0 sind. Bezeichnet man dieselbe mit $P(z^0)$ und den grössten Theiler, welchen $P(z^0)$ mit $G_1^0(z^0)$ im Sinne der Congruenz mod. $(\mathfrak{M})$ gemein hat, mit $W(z^0)$, so kann nach art. III, § 5 meiner Abhandlung „über einige Anwendungen der Modulsysteme etc.[1])“ angenommen werden, dass die Coefficienten von $W(z^0)$ ebenfalls rationale Functionen der Grössen $\mathfrak{R}$ und u^0 sind. Da nun $W(z^0)$, mod. $(\mathfrak{M})$ betrachtet, ein Theiler der Function $G_1^0(z^0)$ und diese wiederum ein Theiler der Function $G^0(z^0)$ ist, so muss eine Congruenz:

$$G^0(z^0, c_1, c_2, \ldots c_n) \equiv W(z^0)\, V(z^0) \pmod{(\mathfrak{M})}$$

bestehen, in welcher G^0 — wie im Anfange dieses Paragraphen — die *Galois*'sche Function und $V(z^0)$ eine ganze Function von z^0 bedeutet, deren Coefficienten rationale Functionen der Grössen $\mathfrak{R}$ und u^0 sind. Da aber das Modulsystem $(\mathfrak{M})$ nur aus den Elementen:

$$G_1(z), \ldots, \quad x_k \psi(\ldots c_h, \ldots) - \varphi_k(z; \ldots c_h, \ldots), \quad \ldots \qquad (h, k = 1, 2, \ldots n)$$

[1]) Band III S. 190—194 dieser Ausgabe. H.

besteht, und in jener Congruenz $G^0(z^0) \equiv W(z^0)\, V(z^0)$ weder die Variable z noch die Variabeln $x_1, x_2, \ldots x_n$ vorkommen, so muss die *Gleichung:*

$$G^0(z^0, c_1, c_2, \ldots c_n) = W(z^0)\, V(z^0)$$

bestehen, welche mit der Voraussetzung, dass $G_1(z^0)$ einer der *irreductibeln* Factoren von $G^0(z^0)$ ist, in Widerspruch stehen würde, wenn $W(z^0)$ in Beziehung auf z^0 von niedrigerem Grade wäre als $G_1^0(z^0)$. Nun ist aber $W(z^0)$, mod. $(\mathfrak{M})$ betrachtet, der grösste gemeinsame Theiler der Functionen $G_1^0(z^0)$ und $P(z^0)$, welche beide in Beziehung auf z^0 von demselben Grade r sind. Es muss also $W(z^0)$, da es von eben demselben Grade r sein muss, sowohl mit $P(z^0)$ als auch mit $G_1^0(z^0)$ für das Modulsystem $(\mathfrak{M})$ congruent sein. Daher muss:

$$P(z^0) \equiv G_1^0(z^0) \pmod{(\mathfrak{M})}$$

oder:

$$\prod_g (z^0 - \theta_h^{(k)}(z_g^0)) \equiv \prod_g (z^0 - z_g^0) \pmod{(\mathfrak{M})} \qquad (g, h, k = 1, 2, \ldots r)$$

sein und demnach

> $\theta_h^{(k)}(z_g^0)$ für jeden der r Werthe $g = 1, 2, \ldots r$ mit je einer der Grössen $z_1^0, z_2^0, \ldots z_r^0$ mod. $(\mathfrak{M})$ übereinstimmen.

Da die Functionen $\theta_h^{(k)}$ also eine Gruppe bilden, so bilden auch die Permutationen $(r_1, r_2, \ldots r_n)$ eine Gruppe, und es giebt daher eine Functionen-Gattung $\mathfrak{g}(x_1, x_2, \ldots x_n)$, zu welcher diese Permutationen gehören. Setzt man in der obigen Congruenz (8.) für $z^0, u_1^0, u_2^0, \ldots u_n^0$ irgend welche unter einander verschiedene ganze Zahlen, so wird $G_1^0(z^0)$ eine Grösse des Rationalitätsbereichs $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$, welche mit c bezeichnet werden möge, und das Product auf der rechten Seite wird offenbar eine ganze ganzzahlige Function von $x_1, x_2, \ldots x_n$, welche mit $\mathfrak{g}(x_1, x_2, \ldots x_n)$ bezeichnet werden möge. Es resultirt daher eine Congruenz:

$$(11.) \qquad \mathfrak{g}(x_1, x_2, \ldots x_n) \equiv c \pmod{(\mathfrak{M})},$$

in welcher $\mathfrak{g}$ die Gattung repräsentirt, welche durch jeden der irreductibeln Factoren der *Galois*'schen Function von $F(x)$ bestimmt wird. Diese irreductibeln Factoren sind sämmtlich von gleichem Grade, und die Gradzahl selbst ist gleich der Anzahl der Permutationen der Gattung $\mathfrak{g}$.

Bedeutet $\Phi(y, \mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n) = 0$, wie oben im § 3, die Gleichung, welcher $\mathfrak{g}(x_1, x_2, \ldots x_n)$ genügt, so ist:

$$\Phi(\mathfrak{g}(x_1, x_2, \ldots x_n), \mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n) = 0,$$

und da:

$$\mathfrak{g}(x_1, x_2, \ldots x_n) \equiv c, \quad \mathfrak{f}_1 \equiv c_1, \quad \mathfrak{f}_2 \equiv c_2, \quad \ldots \mathfrak{f}_n \equiv c_n \pmod{(\mathfrak{M})}$$

ist, so muss $\Phi(c, c_1, c_2, \ldots c_n)$ für das Modulsystem $(\mathfrak{M})$ congruent Null sein. Die $n+1$ Variabeln $z, x_1, x_2, \ldots x_n$, aus denen die $n+1$ Elemente des Modulsystems $(\mathfrak{M})$ gebildet sind, kommen aber in $\Phi(c, c_1, c_2, \ldots c_n)$ nicht vor; es ist daher ebenso wie oben zu erschliessen, dass die *Gleichung*:

$$\Phi(c, c_1, c_2, \ldots c_n) = 0$$

bestehen muss.

§ 5.

Wendet man die Entwickelungen, welche am Schlusse des § 3 an die mit (5.) bezeichnete Congruenz geknüpft worden sind, auf die Congruenz (11.) des § 4 an, in welcher $\mathfrak{g}$ die dort hervorgehobene besondere Bedeutung hat, so zeigt sich, dass für das Modulsystem $(\mathfrak{M})$ die Congruenzen:

$$(11^*.) \qquad \mathfrak{f}_1 \equiv c_1, \ \mathfrak{f}_2 \equiv c_2, \ \ldots \mathfrak{f}_n \equiv c_n; \ \mathfrak{g}' \equiv c', \ \mathfrak{g}'' \equiv c'', \ \mathfrak{g}''' \equiv c''', \ \ldots$$

erfüllt sind, und es ergiebt sich demnach als ein Hauptresultat,

dass das Modulsystem $(\mathfrak{M})$ in dem Modulsysteme:

$$(\mathfrak{M}_\mathfrak{g}) \qquad (\mathfrak{f}_1 - c_1, \ \mathfrak{f}_2 - c_2, \ \ldots \mathfrak{f}_n - c_n; \ \mathfrak{g}' - c', \ \mathfrak{g}'' - c'', \ \mathfrak{g}''' - c''', \ \ldots)$$

enthalten ist, wenn $\mathfrak{g}', \mathfrak{g}'', \mathfrak{g}''', \ldots$ die Elemente eines Fundamentalsystems der Gattung bedeuten, welche durch einen der irreductibeln Factoren der von $F(x)$ abgeleiteten *Galois*'schen Function bestimmt wird.

Es soll nun erstens gezeigt werden, dass dieses Resultat noch Geltung behält, wenn dem Modulsysteme $(\mathfrak{M}_\mathfrak{g})$ das Element:

$$z - u_1 x_1 - u_2 x_2 - \cdots - u_n x_n$$

hinzugefügt wird, und es soll dann zweitens gezeigt werden, dass auch umgekehrt das Modulsystem $(\mathfrak{M}_\mathfrak{g})$ bei Hinzufügung dieses neuen Elementes in dem Modulsysteme $(\mathfrak{M})$ enthalten ist.

Aus der Congruenz (2**.) im § 2 folgt unmittelbar, dass:

$$\psi(\ldots \mathfrak{f}_h, \ldots) \sum_k u_k x_k \equiv \sum_{(h,\, k=1,\, 2,\, \ldots\, n)} u_k \varphi_k(z; \ldots \mathfrak{f}_h, \ldots) \pmod{z - u_1 x_1 - u_2 x_2 - \cdots - u_n x_n}$$

wird, oder also:

$$z\psi(\ldots \mathfrak{f}_h, \ldots) \equiv \sum_{(h,\, k=1,\, 2,\, \ldots\, n).} u_k \varphi_k(z; \ldots \mathfrak{f}_h, \ldots) \pmod{z - u_1 x_1 - u_2 x_2 - \cdots - u_n x_n}$$

Diese Congruenz behält aber ihre Geltung auch für *jeden* Modul:

$$z - u_1 x_{i_1} - u_2 x_{i_2} - \cdots - u_n x_{i_n},$$

und es ist daher:

$$(12.) \qquad z\psi(\ldots \mathfrak{f}_h, \ldots) \equiv \sum_{(h,\, k=1,\, 2,\, \ldots\, n),} u_k \varphi_k(z; \ldots \mathfrak{f}_h, \ldots) \pmod{G(z, \mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n)}$$

also ferner

(12*.) $$z\psi(\dots c_h, \dots) \equiv \sum_k u_k \varphi_k(z; \dots c_h, \dots) \pmod{G_1(z)} \qquad (h, k = 1, 2, \dots n).$$

Nun besteht offenbar die Congruenz:

$$(z - \sum_k u_k x_k)\psi(\dots c_h, \dots) \equiv z\psi(\dots c_h, \dots) - \sum_k u_k \varphi_k(z; \dots c_h, \dots) \qquad (h, k = 1, 2, \dots$$

für das aus den Elementen:

$$x_k\psi(\dots c_h, \dots) - \varphi_k(z; \dots c_h, \dots) \qquad (h, k = 1, 2, \dots n)$$

gebildete Modulsystem. Es sind dies auch die letzten n Elemente des Modulsystems $(\mathfrak{M})$. Der Ausdruck auf der rechten Seite dieser Congruenz ist aber für den Modul $G_1(z)$, der das erste Element des Modulsystems $(\mathfrak{M})$ ist, in Gemässheit der Congruenz (12*.) congruent Null; es ist daher auch:

$$(z - \sum_k u_k x_k)\psi(\dots c_h, \dots) \equiv 0 \pmod{(\mathfrak{M})} \qquad (h, k = 1, 2, \dots n),$$

und hieraus ergiebt sich unmittelbar die Congruenz:

$$z - u_1 x_1 - u_2 x_2 - \cdots - u_n x_n \equiv 0 \pmod{(\mathfrak{M})},$$

deren Richtigkeit nachgewiesen werden sollte.

In Beziehung auf den nunmehr zu führenden Nachweis, dass jedes der Elemente des Modulsystems $(\mathfrak{M})$ das aus den Elementen:

$$\mathfrak{f}_1 - c_1, \ \mathfrak{f}_2 - c_2, \dots \mathfrak{f}_n - c_n; \ \mathfrak{g}' - c', \ \mathfrak{g}'' - c'', \ \mathfrak{g}''' - c''', \dots; \ z - u_1 x_1 - u_2 x_2 - \cdots - u_n x_n$$

gebildete Modulsystem enthält, bemerke ich zuvörderst, dass sich dies für die letzten n Elemente des Modulsystems $(\mathfrak{M})$:

$$x_k\psi(\dots c_h, \dots) - \varphi_k(z; \dots c_h, \dots) \qquad (h, k = 1, 2, \dots n)$$

schon aus der Congruenz (2*.) des § 2 ergiebt, gemäss welcher offenbar:

$$x_k\psi(\dots c_h, \dots) \equiv \varphi_k(z; \dots c_h, \dots) \pmod{z - u_1 x_1 - u_2 x_2 - \cdots - u_n x_n;\ \mathfrak{f}_1 - c_1, \dots \mathfrak{f}_n - c_n} \qquad (h, k = 1, 2, \dots n)$$

wird. Es ist also nur noch nachzuweisen, dass $G_1(z) \equiv 0 \pmod{(\mathfrak{M}_0)}$ wird, oder also dass die Congruenz:

(13.) $$G_1(u_1 x_1 + u_2 x_2 + \cdots + u_n x_n) \equiv 0$$

$$(\text{modd. } \mathfrak{f}_1 - c_1, \ \mathfrak{f}_2 - c_2, \dots \mathfrak{f}_n - c_n; \ \mathfrak{g}' - c', \ \mathfrak{g}'' - c'', \dots)$$

besteht.

Die Richtigkeit dieser Congruenz erhellt nun gemäss der Ausführung am Schlusse des § 20 meiner mehrerwähnten Festschrift einfach daraus, dass, wie im § 11 derselben gezeigt ist, $G_1(u_1 x_1 + u_2 x_2 + \cdots + u_n x_n)$ für alle diejenigen Werthsysteme $x_1 = \xi_{r_1}, \ x_2 = \xi_{r_2}, \dots x_n = \xi_{r_n}$ gleich Null wird, für welche die Gleichungen:

(14.) $$\mathfrak{f}_1 = c_1, \ \mathfrak{f}_2 = c_2, \dots \mathfrak{f}_n = c_n; \ \mathfrak{g}' = c', \ \mathfrak{g}'' = c'', \ \mathfrak{g}''' = c''', \dots$$

befriedigt werden, d. h. dass die Resolvente dieses Gleichungssystems durch:

$$G_1(u_1 x_1 + u_2 x_2 + \cdots + u_n x_n) = 0$$

dargestellt wird. Hier bedeuten $\xi_1, \xi_2, \dots \xi_n$, wie a. a. O., die n Wurzeln der Gleichung $F(x) = 0$. Aber man wird eben, wie schon oben erwähnt ist, mittels der Congruenz (3**.) des § 2 oder auch mittels der Congruenz (4*.) des § 3 der Einführung der algebraischen Grössen enthoben und braucht an Stelle des Gleichungssystems (14.) nur das oben mit (11*.) bezeichnete System der Congruenzen, unter Hinzufügung der Congruenz:

$$z \equiv u_1 x_1 + u_2 x_2 + \cdots + u_n x_n,$$

d. h. also das System von Congruenzen:

$$(15.)\qquad \begin{cases} \mathfrak{f}_1 \equiv c_1,\ \mathfrak{f}_2 \equiv c_2,\ \dots\ \mathfrak{f}_n \equiv c_n;\ \mathfrak{g}' \equiv c',\ \mathfrak{g}'' \equiv c'',\ \dots; \\ z \equiv u_1 x_1 + u_2 x_2 + \cdots + u_n x_n \pmod{(\mathfrak{M})} \end{cases}$$

zu Grunde zu legen, deren Richtigkeit oben nachgewiesen worden ist, um ohne die Vermittelung algebraischer Grössen das Bestehen der Congruenz (13.) zu erschliessen. Dies soll im folgenden Paragraphen ausgeführt werden.

§ 6.

Bildet man die $n+1$ Functionen von $x_1, x_2, \dots x_n$:

$$u_1 x_1 + u_2 x_2 + \cdots + u_n x_n - z,$$

$$v'_h(\mathfrak{f}_1 - c_1) + v''_h(\mathfrak{f}_2 - c_2) + \cdots + v_h^{(n)}(\mathfrak{f}_n - c_n) + w'_h(\mathfrak{g}' - c') + w''_h(\mathfrak{g}'' - c'') + w'''_h(\mathfrak{g}''' - c''') + \cdots \quad (h = 1, 2, \dots n),$$

wo $u'_h, v''_h, \dots w'_h, w''_h, \dots$ Unbestimmte bedeuten, so wird deren Resultante eine ganze ganzzahlige Function von $z, c_1, c_2, \dots c_n, c', c'', c''', \dots$ und den Unbestimmten u, v, w. Bezeichnet man nun den grössten von den Unbestimmten:

$$v'_h,\ v''_h,\ \dots v_h^{(n)},\ w'_h,\ w''_h,\ w'''_h,\ \dots \qquad (h = 1, 2, \dots n)$$

unabhängigen Theiler dieser Resultante mit $\overline{G}(z)$, so erschliesst man genau so wie im § 20 S. 75 meiner erwähnten Festschrift[1]), dass $\overline{G}(z)$ das Modulsystem enthält, dessen Elemente die Functionen:

$$u_1 x_1 + u_2 x_2 + \cdots + u_n x_n - z;\ \mathfrak{f}_1 - c_1,\ \mathfrak{f}_2 - c_2,\ \dots\ \mathfrak{f}_n - c_n;\ \mathfrak{g}' - c',\ \mathfrak{g}'' - c'',\ \mathfrak{g}''' - c''', \dots$$

sind. Da aber jedes dieser Elemente gemäss den Congruenzen (15.) das Modulsystem $(\mathfrak{M})$ enthält, so muss die Congruenz $\overline{G}(z) \equiv 0 \pmod{(\mathfrak{M})}$ bestehen, welche sich offenbar auf eine Congruenz für das erste Element des Modulsystems $(\mathfrak{M})$:

[1]) Bd. II S. 332—333 dieser Ausgabe. H.

$$(16.)\qquad \overline{G}(z) \equiv 0 \pmod{G_1(z)}$$

reducirt, da die Function $\overline{G}(z)$ von den Variabeln x, die in den übrigen Elementen vorkommen, unabhängig ist.

Gemäss den obigen Entwickelungen in den §§ 2 und 3 lassen sich stets Primmodulsysteme bestimmen, für welche diejenige Function, welche, gleich Null gesetzt, die Resolvente eines Systems von n Gleichungen mit n Unbekannten repräsentirt, einem Product von Linearfactoren congruent wird. Die n Gleichungen selbst werden also, als Congruenzen für eben dieses Primmodulsystem aufgefasst, durch so viel Werthsysteme der Unbekannten befriedigt, als die Anzahl jener Linearfactoren beträgt. Bezeichnet man mit $\Gamma(z)$ einen zur Zerlegung der Resolvente des Systems:

$$F_h(x_1, x_2, \dots x_n) = 0 \qquad (h = 1, 2, \dots n)$$

geeigneten Primmodul und mit

$$\xi_{1k}, \xi_{2k}, \dots \xi_{nk} \qquad (k = 1, 2, \dots r)$$

die Werthe, für welche die n Congruenzen:

$$F_h(\xi_{1k}, \xi_{2k}, \dots \xi_{nk}) \equiv 0 \pmod{\Gamma(z)} \qquad \begin{pmatrix} h = 1, 2, \dots n \\ k = 1, 2, \dots r \end{pmatrix}$$

erfüllt sind, so kann die Resultante der $n+1$ Functionen:

$$F_0(x_1, x_2, \dots x_n),\ F_1(x_1, x_2, \dots x_n), \dots F_n(x_1, x_2, \dots x_n)$$

mit Hülfe des Products:

$$\prod_k F_0(\xi_{1k}, \xi_{2k}, \dots \xi_{nk}) \qquad (k = 1, 2, \dots r)$$

gebildet werden. Dieses Product ist eine ganze Function von z, deren Coefficienten demselben Rationalitätsbereich angehören wie die Coefficienten

der Functionen F, und welche als symmetrische Function der Werthsysteme $\xi_{1k}, \xi_{2k}, \ldots \xi_{nk}$, im Sinne der Congruenz modulo $\Gamma(z)$, von z unabhängig ist. Der Rest der Division durch $\Gamma(z)$ ist daher eine rationale Function der Grössen, welche den Rationalitätsbereich der Coefficienten von $F_0, F_1, \ldots F_n$ bilden. Sind nun diese $n+1$ Functionen *vollständige* ganze Functionen (gewisser Dimensionen) von $x_1, x_2, \ldots x_n$, deren verschiedene Coefficienten selbst die Elemente des Rationalitätsbereichs repräsentiren, so ist der Zähler jenes Restes der Division durch $\Gamma(z)$ diejenige ganze ganzzahlige Function der Coefficienten von $F_0, F_1, \ldots F_n$, welche als die Resultante des Functionensystems $(F_0, F_1, \ldots F_n)$ zu bezeichnen ist.

Mit Hülfe der so definirten Resultante kann die Resolvente eines Systems von $n+1$ Congruenzen mit $n+1$ Unbekannten:

$$\Phi_k(x_0, x_1, \ldots x_n) \equiv 0 \qquad (k=0, 1, \ldots n)$$

gebildet werden, indem erst $x_0 = x - u_1 x_1 - u_2 x_2 - \cdots - u_n x_n$ und ferner:

$$\Phi_k(x - u_1 x_1 - u_2 x_2 - \cdots - u_n x_n, x_1, x_2, \ldots x_n) = F_k(x_1, x_2, \ldots x_n) \qquad (k=0, 1, \ldots n)$$

gesetzt wird. Die Resolvente wird alsdann eine ganze Function von x, mit deren Hülfe wieder in der oben angegebenen Weise die Resultante eines Systems von $n+2$ Functionen mit $n+1$ Variabeln definirt werden kann.

Nach der angegebenen Bildungsweise der Resultante muss $\overline{G}(z)$, abgesehen von einem von z unabhängigen Factor, dem Producte aller derjenigen Linearfactoren $z - u_1\xi_1 - u_2\xi_2 - \cdots - u_n\xi_n$ congruent sein, für welche die Congruenzen:

$$(17.) \qquad \mathfrak{f}_1 \equiv c_1, \ \mathfrak{f}_2 \equiv c_2, \ \ldots \mathfrak{f}_n \equiv c_n; \ \mathfrak{g}' \equiv c', \ \mathfrak{g}'' \equiv c'', \ \mathfrak{g}''' \equiv c''', \ \ldots$$

erfüllt sind, wenn in den Functionen $\mathfrak{f}$ und $\mathfrak{g}$ die Variabeln $x_1, x_2, \ldots x_n$ beziehungsweise durch $\xi_1, \xi_2, \ldots \xi_n$ ersetzt werden. Hierbei kann man als Modulsystem dasjenige nehmen, welches entsteht, wenn man in dem mit $(\mathfrak{M})$ bezeichneten Modulsystem die Variable z durch eine andere, z. B. z^0 ersetzt,

um sie nicht mit der in den Linearfactoren vorkommenden Variabeln z zu confundiren. Die Grössen ξ sind dann ganze Functionen von z^0, und da gemäss den Congruenzen $\mathfrak{f}_1 \equiv c_1, \ \mathfrak{f}_2 \equiv c_2, \ \ldots \mathfrak{f}_n \equiv c_n$:

$$\xi_1 + \xi_2 + \cdots + \xi_n \equiv c_1, \ \ \xi_1\xi_2 + \xi_1\xi_3 + \cdots + \xi_{n-1}\xi_n \equiv c_2, \ \cdots \ \ \xi_1\xi_2 \cdots \xi_n \equiv c_n,$$

also für ein unbestimmtes x:

$$(x - \xi_1)(x - \xi_2) \cdots (x - \xi_n) \equiv F(x)$$

sein muss, so besteht für je zwei verschiedene Werthsysteme $\xi_1, \xi_2, \ldots \xi_n$ und $\xi_1', \xi_2', \ldots \xi_n'$ die Relation:

$$(x - \xi_1)(x - \xi_2) \cdots (x - \xi_n) \equiv (x - \xi_1')(x - \xi_2') \cdots (x - \xi_n'),$$

aus welcher hervorgeht, dass die Grössen ξ mit den Grössen ξ' (abgesehen von der Reihenfolge) übereinstimmen. Die Werthsysteme, welche den Congruenzen (17.) genügen, sind hiernach in folgender Weise darzustellen:

$$x_{r_1} = \xi_1, \ \ x_{r_2} = \xi_2, \ \ldots \ x_{r_n} = \xi_n,$$

wo $r_1, r_2, \ldots r_n$ eine Permutation der Zahlen $1, 2, \ldots n$ bedeutet, und es treten dabei offenbar alle Permutationen der durch das Functionensystem $\mathfrak{g}', \mathfrak{g}'', \mathfrak{g}''', \ldots$ repräsentirten Gattung auf, aber auch keine andern.

Hiermit ist nachgewiesen, dass der Grad der Function $\overline{G}(z)$ mit der Anzahl der Permutionen der Gattung $(\mathfrak{g}', \mathfrak{g}'', \mathfrak{g}''', \ldots)$ übereinstimmt. Da aber diese Anzahl, wie schon oben nach Herleitung der Congruenz (11.) bemerkt worden, wiederum gleich dem Grade des mit $G_1(z)$ bezeichneten irreductibeln Factors der *Galois*'schen Function von $F(x)$ ist, so müssen die beiden Functionen $\overline{G}(z)$ und $G_1(z)$ von gleichem Grade und folglich, wegen der Congruenz (16.), mit einander *identisch* sein.

Nun ist schon oben gezeigt worden, dass das Modulsystem:

$$u_1x_1 + u_2x_2 + \cdots + u_nx_n - z;\ \mathfrak{f}_1 - c_1,\ \mathfrak{f}_2 - c_2, \ldots \mathfrak{f}_n - c_n;$$
$$\mathfrak{g}' - c',\ \mathfrak{g}'' - c'',\ \mathfrak{g}''' - c''', \ldots$$

in der Function $\overline{G}(z)$ enthalten, d. h. also, dass die Congruenz:

$$\overline{G}(u_1x_1 + u_2x_2 + \cdots + u_nx_n) \equiv 0$$
$$(\text{modd. } \mathfrak{f}_1 - c_1,\ \mathfrak{f}_2 - c_2, \ldots \mathfrak{f}_n - c_n;\ \mathfrak{g}' - c',\ \mathfrak{g}'' - c'',\ \mathfrak{g}''' - c''', \ldots)$$

erfüllt ist. Da sich nun jetzt die Function $G_1(z)$ als mit der Function $\overline{G}(z)$ identisch erwiesen hat, ist der Nachweis für die Richtigkeit der oben mit (13.) bezeichneten Congruenz erbracht.

§ 7.

In den beiden vorhergehenden Paragraphen ist die Aequivalenz der zwei Modulsysteme:

$$(\mathfrak{M}) \qquad (G_1(z); \ldots, x_k\psi(\ldots c_k, \ldots) - \varphi_k(z; \ldots c_k, \ldots), \ldots) \qquad (k = 1, 2, \ldots n),$$

$$(\mathfrak{M}') \qquad \begin{cases} (\mathfrak{f}_1 - c_1,\ \mathfrak{f}_2 - c_2, \ldots \mathfrak{f}_n - c_n;\ \mathfrak{g}' - c',\ \mathfrak{g}'' - c'',\ \mathfrak{g}''' - c''', \ldots; \\ \qquad z - u_1x_1 - u_2x_2 - \cdots - u_nx_n) \end{cases}$$

dargethan worden.

Aus dieser Aequivalenz folgt, dass die Congruenz (5.) im § 3:

$$\mathfrak{g}(x_1,\ x_2, \ldots x_n) \equiv c \pmod{(\mathfrak{M})}$$

auch *modulo* $(\mathfrak{M}')$ gelten muss, und — da die Ausdrücke auf beiden Seiten der Congruenz unabhängig von z sind — auch für das Modulsystem $(\mathfrak{M}_\mathfrak{g})$ des § 5. Für jede ganze Function $\mathfrak{g}$, für welche die entsprechende Gleichung $\Phi(\mathfrak{g}, c_1, c_2, \ldots c_n) = 0$ eine rationale Wurzel $\mathfrak{g} = c$ hat, muss also eine

Congruenz $\mathfrak{g} \equiv c \pmod{(\mathfrak{M}_\mathfrak{g})}$ bestehen, und es kann daher die Differenz $\mathfrak{g} - c$ den Elementen:

$$\mathfrak{f}_1 - c_1,\ \mathfrak{f}_2 - c_2, \ldots \mathfrak{f}_n - c_n;\ \mathfrak{g}' - c',\ \mathfrak{g}'' - c'',\ \mathfrak{g}''' - c''', \ldots$$

des Modulsystems $(\mathfrak{M}_\mathfrak{g})$ hinzugefügt werden, ohne dasselbe zu verändern.

Es seien nun, wie am Ende des § 3:

$$\mathfrak{g}_0'(x_1,\ x_2, \ldots x_n),\ \mathfrak{g}_0''(x_1,\ x_2, \ldots x_n),\ \mathfrak{g}_0'''(x_1,\ x_2, \ldots x_n), \ldots$$

die Elemente eines Fundamentalsystems einer Gattung von Functionen, für welche die identischen Gleichungen:

$$\Phi'(\mathfrak{g}_0',\ \mathfrak{f}_1,\ \mathfrak{f}_2, \ldots \mathfrak{f}_n) = 0,\quad \Phi''(\mathfrak{g}_0'',\ \mathfrak{f}_1,\ \mathfrak{f}_2, \ldots \mathfrak{f}_n) = 0, \ldots$$

bestehen, und zwar sei dies die Gattung *höchster* Ordnung, für welche die Gleichungen:

$$\Phi'(\mathfrak{g}_0',\ c_1,\ c_2, \ldots c_n) = 0,\quad \Phi''(\mathfrak{g}_0'',\ c_1,\ c_2, \ldots c_n) = 0, \ldots$$

rationale Wurzeln $\mathfrak{g}_0' = c_0'$, $\mathfrak{g}_0'' = c_0''$, ... zulassen. Alsdann bleibt nach den obigen Entwickelungen das Modulsystem $(\mathfrak{M}_\mathfrak{g})$ bei Hinzufügung der Elemente $\mathfrak{g}_0' - c_0'$, $\mathfrak{g}_0'' - c_0''$, $\mathfrak{g}_0''' - c_0'''$, ... ungeändert. Es ist aber im Anfange des § 5 das Modulsystem $(\mathfrak{M}_\mathfrak{g})$ dadurch charakterisirt worden, dass die Functionen $\mathfrak{g}'$, $\mathfrak{g}''$, $\mathfrak{g}'''$, ... bei den zu den Elementen:

$$\mathfrak{f}_1 - c_1,\ \mathfrak{f}_2 - c_2,\ \mathfrak{f}_3 - c_3, \ldots \mathfrak{f}_n - c_n$$

hinzugefügten Elementen:

$$\mathfrak{g}' - c',\ \mathfrak{g}'' - c'',\ \mathfrak{g}''' - c''', \ldots$$

ein Fundamentalsystem derjenigen Gattung bilden, welche durch die irreductibeln Factoren der *Galois*'schen Function von $F(x)$ bestimmt werden.

Diese Gattung $(\mathfrak{g}', \mathfrak{g}'', \mathfrak{g}''', \ldots)$ muss also die Gattung $(\mathfrak{g}_0', \mathfrak{g}_0'', \mathfrak{g}_0''', \ldots)$ unter sich enthalten. Denn sonst würde eine dritte Gattung (G), welche diese beiden Gattungen unter sich enthält, durch lineare Verbindungen:

$$a\mathfrak{g}^{(k)} + \mathfrak{g}_0^{(k)} \qquad (k, k=1, 2, \ldots),$$

in welchen a eine ganze Zahl bedeutet, charakterisirt werden können, und es würden vermöge der Congruenz:

$$a\mathfrak{g}^{(k)} + \mathfrak{g}_0^{(k)} \equiv ac^{(k)} + c_0^{(k)} \pmod{(\mathfrak{M}_\mathfrak{g})}$$

an die Stelle der Elemente $\mathfrak{g}' - c'$, $\mathfrak{g}'' - c''$, $\mathfrak{g}''' - c'''$, ... in dem Modulsysteme $(\mathfrak{M}_\mathfrak{g})$ solche Elemente:

$$G' - C', \quad G'' - C'', \quad G''' - C''', \ldots$$

gesetzt werden können, in welchen G', G'', G''', ... einer Gattung höherer Ordnung angehören als diejenige, deren Fundamentalsystem $\mathfrak{g}'$, $\mathfrak{g}''$, $\mathfrak{g}'''$, ... ist.

Am Schlusse des § 4 ist gezeigt worden, dass die Gattung $(\mathfrak{g}', \mathfrak{g}'', \mathfrak{g}''', \ldots)$ selbst eine derjenigen Gattungen ist, für welche die Gleichungen:

$$\Phi(\mathfrak{g}, c_1, c_2, \ldots c_n) = 0$$

eine rationale Wurzel $\mathfrak{g} = c$ haben, wenn

$$\Phi(\mathfrak{g}(x_1, x_2, \ldots x_n), \mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n) = 0$$

die identische Gleichung ist, welcher eine der Gattung $(\mathfrak{g}', \mathfrak{g}'', \mathfrak{g}''', \ldots)$ angehörige Function $\mathfrak{g}(x_1, x_2, \ldots x_n)$ genügt. Der Voraussetzung nach ist aber $(\mathfrak{g}_0', \mathfrak{g}_0'', \mathfrak{g}_0''', \ldots)$ die Gattung höchster Ordnung unter allen diesen Gattungen. Ihre Ordnung kann also nicht kleiner als die Ordnung der Gattung $(\mathfrak{g}', \mathfrak{g}'', \mathfrak{g}''', \ldots)$ sein, und die Gattung $(\mathfrak{g}_0', \mathfrak{g}_0'', \mathfrak{g}_0''', \ldots)$ muss daher, da sie — wie so eben gezeigt worden — unter der Gattung $(\mathfrak{g}', \mathfrak{g}'', \mathfrak{g}''', \ldots)$

enthalten und doch von nicht kleinerer Ordnung ist, mit eben dieser Gattung $(\mathfrak{g}', \mathfrak{g}'', \mathfrak{g}''', \ldots)$ identisch sein.

Die durch die irreductibeln rationalen Factoren der Galois'schen Function $G(z, c_1, c_2, \ldots c_n)$ bestimmte Gattung, welche durch die Gesammtheit der Elemente des Modulsystems $(\mathfrak{M}_\mathfrak{g})$ repräsentirt wird, ist also zugleich die Gattung höchster Ordnung, für welche die definirende Gleichung eine rationale Wurzel hat.

Hiermit ist die am Schlusse des § 3 charakterisirte Gattung in der Weise bestimmt, wie es im Anfange des § 4 angekündigt worden ist.

Aus der Aequivalenz der Modulsysteme $(\mathfrak{M})$ und $(\mathfrak{M}')$ folgt aber ferner, da das erstere sich als ein Primmodulsystem erwiesen hat, dass auch das letztere ein Primmodulsystem ist, und da dieses offenbar dieselbe Eigenschaft behält, wenn man das letzte Element $z - u_1x_1 - u_2x_2 - \cdots - u_nx_n$ weglässt, so ergiebt sich das Hauptresultat, dass das mit $(\mathfrak{M}_\mathfrak{g})$ bezeichnete Modulsystem:

$$(\mathfrak{f}_1 - c_1, \mathfrak{f}_2 - c_2, \ldots \mathfrak{f}_n - c_n; \mathfrak{g}' - c', \mathfrak{g}'' - c'', \mathfrak{g}''' - c''', \ldots)$$

ein in dem Modulsysteme:

$$(\mathfrak{f}_1 - c_1, \mathfrak{f}_2 - c_2, \ldots \mathfrak{f}_n - c_n)$$

enthaltenes *Prim*modulsystem ist, für welches gemäss § 1 die Congruenz:

$$(1^{**}.) \qquad x^n - c_1x^{n-1} + c_2x^{n-2} - \cdots \pm c_n \equiv (x - x_1)(x - x_2)\cdots(x - x_n)$$

besteht. Durch die Bestimmung des Primmodulsystems $(\mathfrak{M}_\mathfrak{g})$ wird die in der Einleitung gestellte Aufgabe noch in einer anderen Weise gelöst, als es oben im § 2 geschehen ist, und in vieler Beziehung ist diese letztere Lösung vorzuziehen.

§ 8.

Die in den vorhergehenden Paragraphen entwickelten Resultate können folgendermaassen formulirt werden.

Bedeutet $G(z, \mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n; u_1, u_2, \ldots u_n)$ das über alle $n!$ Permutationen $(i_1, i_2, \ldots i_n)$ erstreckte Product:

$$\Pi(z - u_1 x_{i_1} - u_2 x_{i_2} - \cdots - u_n x_{i_n}),$$

dargestellt als ganze ganzzahlige Function der Variabeln $z, u_1, u_2, \ldots u_n$ und der mit $\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n$ bezeichneten elementaren symmetrischen Functionen von $x_1, x_2, \ldots x_n$, und versteht man unter:

$$G(z, c_1, c_2, \ldots c_n; u_1, u_2, \ldots u_n)$$

„die von der Function:

$$x^n - c_1 x^{n-1} + c_2 x^{n-2} - \cdots \pm c_n$$

abgeleitete Galois'sche Function", in welcher $c_1, c_2, \ldots c_n$ ganze Grössen eines natürlichen Rationalitätsbereichs $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$ sind, so repräsentirt jeder der irreductibeln Factoren von:

$$G(z, c_1, c_2, \ldots c_n; u_1, u_2, \ldots u_n)$$

eine bestimmte Gattung von Functionen der Unbestimmten $u_1, u_2, \ldots u_n$. Es ist dies die *„Affect-Gattung"* der Gleichung:

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

wenn eben diese Gleichung irreductibel ist*).

*) Vgl. § 12, S. 36 meiner mehrfach citirten Festschrift[1]).

[1]) Band II S. 287 dieser Ausgabe. H.

Bilden nun die ganzen ganzzahligen Functionen von $u_1, u_2, \ldots u_n$:

$$\mathfrak{g}'(u_1, u_2, \ldots u_n), \mathfrak{g}''(u_1, u_2, \ldots u_n), \mathfrak{g}'''(u_1, u_2, \ldots u_n), \ldots$$

ein Fundamentalsystem der Affect-Gattung, so ist jede ganze ganzzahlige Function von $x_1, x_2, \ldots x_n$, welche dem durch das Functionensystem:

$$(\mathfrak{g}'(x_1, x_2, \ldots x_n), \mathfrak{g}''(x_1, x_2, \ldots x_n), \mathfrak{g}'''(x_1, x_2, \ldots x_n), \ldots)$$

charakterisirten Gattungsbereich angehört, als ganze homogene lineare Function von:

$$\mathfrak{g}'(x_1, x_2, \ldots x_n), \mathfrak{g}''(x_1, x_2, \ldots x_n), \mathfrak{g}'''(x_1, x_2, \ldots x_n), \ldots$$

darstellbar, deren Coefficienten ganze ganzzahlige Functionen der elementaren symmetrischen Functionen $\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n$ sind. Bezeichnet man mit $\mathfrak{g}(x_1, x_2, \ldots x_n)$ irgend eine solche Function, so genügt dieselbe einer identischen Gleichung:

$$\Phi(\mathfrak{g}, \mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n) = 0,$$

wo Φ eine ganze ganzzahlige irreductible Function von $\mathfrak{g}, \mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n$ bedeutet, deren Grad in Beziehung auf $\mathfrak{g}$ gleich der Ordnung der Function $\mathfrak{g}$, also ein Divisor der Ordnung der Gattung $(\mathfrak{g}', \mathfrak{g}'', \mathfrak{g}''', \ldots)$ ist. Die Gleichung:

$$\Phi(\mathfrak{g}, c_1, c_2, \ldots c_n) = 0$$

wird durch einen „rationalen" Werth $\mathfrak{g} = c$ befriedigt, d. h. durch einen solchen, der zum Rationalitätsbereich $(\mathfrak{R}', \mathfrak{R}'', \ldots \mathfrak{R}^{(n-1)})$ gehört. Bedeuten $c', c'', c''', \ldots$ beziehungsweise die rationalen Wurzeln der zu den Functionen $\mathfrak{g}', \mathfrak{g}'', \mathfrak{g}''', \ldots$ gehörigen Gleichungen, und ist:

$$\mathfrak{g}(x_1, x_2, \ldots x_n) = \varphi'(\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n)\mathfrak{g}'(x_1, x_2, \ldots x_n) + \varphi''(\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n)\mathfrak{g}''(x_1, x_2, \ldots x_n) + \cdots,$$

wo $\varphi', \varphi'', \ldots$ ganze ganzzahlige Functionen von $\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_n$ sind, so wird:

$$c = c'\varphi'(c_1, c_2, \dots c_n) + c''\varphi''(c_1, c_2, \dots c_n) + \cdots,$$

und es lassen sich in dieser Weise die rationalen Wurzeln aller derjenigen Gleichungen, welche zu Functionen des Gattungsbereichs $(\mathfrak{g}', \mathfrak{g}'', \mathfrak{g}''', \dots)$ gehören, aus den Wurzeln der zu $\mathfrak{g}', \mathfrak{g}'', \mathfrak{g}''', \dots$ selbst gehörigen Gleichungen bilden. Die Functionen $\mathfrak{g}$ des Gattungsbereichs $(\mathfrak{g}', \mathfrak{g}'', \mathfrak{g}''', \dots)$ sind es aber auch *allein*, für welche die zugehörigen Gleichungen:

$$\Phi(\mathfrak{g}, c_1, c_2, \dots c_n) = 0$$

eine rationale Wurzel $\mathfrak{g} = c$ haben, und die Gattung $(\mathfrak{g}', \mathfrak{g}'', \mathfrak{g}''', \dots)$ kann daher auch eben dadurch definirt werden, dass die zugehörigen Gleichungen rationale Wurzeln haben.

Nach den hier angenommenen Bezeichnungen ist das Modulsystem:

$$(\mathfrak{M}_\mathfrak{g}) \qquad (\mathfrak{f}_1 - c_1, \mathfrak{f}_2 - c_2, \dots \mathfrak{f}_n - c_n;\ \mathfrak{g}' - c', \mathfrak{g}'' - c'', \mathfrak{g}''' - c''', \dots)$$

ein in dem Modulsysteme:

$$(\mathfrak{f}_1 - c_1, \mathfrak{f}_2 - c_2, \dots \mathfrak{f}_n - c_n)$$

enthaltenes *Prim*modulsystem, für welches die Congruenz:

$$x^n - c_1 x^{n-1} + c_2 x^{n-2} - \cdots \pm c_n \equiv (x - x_1)(x - x_2) \cdots (x - x_n)$$

stattfindet, für welches also die Function:

$$x^n - c_1 x^{n-1} + c_2 x^{n-2} - \cdots \pm c_n$$

sich als Product von n linearen Factoren darstellen lässt.

Nach dem *Galois*'schen Princip, wie ich es im § 12 meiner Festschrift zu Herrn *Kummer*'s Doctorjubiläum ausführlich dargelegt habe, tritt an Stelle der Gleichung:

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

wenn deren Wurzeln $\xi_1, \xi_2, \dots \xi_n$ sind, das Gleichungssystem:

$$\mathfrak{f}_k(\xi_1, \xi_2, \dots \xi_n) = c_k,\ \mathfrak{g}'(\xi_1, \xi_2, \dots \xi_n) = c',\ \mathfrak{g}''(\xi_1, \xi_2, \dots \xi_n) = c'', \dots$$
$$(k = 1, 2, \dots n),$$

und jede ganze ganzzahlige Function der n Wurzeln $\xi_1, \xi_2, \dots \xi_n$, welche einen rationalen Werth hat, lässt sich als ganze ganzzahlige Function der Functionen $\mathfrak{f}_1, \mathfrak{f}_2, \dots \mathfrak{f}_n, \mathfrak{g}', \mathfrak{g}'', \mathfrak{g}''', \dots$ und zwar so darstellen, dass sie in Beziehung auf die Functionen $\mathfrak{g}$ linear und homogen wird.

Hier zeigt sich aber eine neue und tiefere Bedeutung des *Galois*'schen Princips darin, dass es in dem Functionensysteme:

$$\mathfrak{f}_k(x_1, x_2, \dots x_n) - c_k,\ \mathfrak{g}'(x_1, x_2, \dots x_n) - c',\ \mathfrak{g}''(x_1, x_2, \dots x_n) - c'', \dots$$
$$(k = 1, 2, \dots n)$$

ein *Prim*modulsystem liefert, für welches die Function:

$$x^n - c_1 x^{n-1} + c_2 x^{n-2} - \cdots \pm c_n$$

dem Producte:

$$(x - x_1)(x - x_2) \cdots (x - x_n)$$

congruent wird. Da nun bei Congruenzen für Primmodulsysteme, genau ebenso wie bei Gleichungen, der Satz gilt, dass ein Product nur dann Null werden kann, wenn einer der Factoren Null ist, so ist jede Deduction, bei welcher die Darstellung einer ganzen Function von x als Product:

$$(x - \xi_1)(x - \xi_2) \cdots (x - \xi_n)$$

verwendet wird, unmittelbar, und ohne dass die Einfachheit irgendwie beeinträchtigt wird, dahin zu modificiren, dass nur die Darstellung als Product:

$$(x - x_1)(x - x_2)\cdots(x - x_n)$$

im Sinne der Congruenz für ein durch das Galois'sche Princip geliefertes Primmodulsystem benutzt wird*). Das *Galois'*sche Princip ist es also, welches die Einführung und Verwendung der algebraischen Grössen überall da entbehrlich macht, wo nicht die Isolirung der unter einander conjugirten algebraischen Grössen, d. h. also die Isolirung der verschiedenen Wurzeln einer irreductibeln Gleichung erfordert wird. Dies geschieht aber z. B. in der arithmetischen Theorie der algebraischen Zahlen, welche in Wahrheit eine Theorie der in Linearfactoren zerfällbaren Formen ist, nur dort, wo die Existenz von Einheiten nachgewiesen wird. Da jedoch die auf die Formen bezüglichen *Resultate*, welche aus der Existenz von Einheiten hergeleitet werden, ohne den Begriff des Algebraischen gefasst werden können, so wird bei einer rationellen Behandlung der arithmetischen Theorie der zerlegbaren Formen vom Begriffe des Algebraischen überhaupt zu abstrahiren und auf Methoden zurückzugehen sein, welche wie die *Gauss'*schen in der V. Section der Disquisitiones arithmeticae den absoluten Rationalitätsbereich der natürlichen Zahlen eigentlich nirgends verlassen.

*) So wird bei der Deduction im § 6 nur die Zerlegung einer ganzen Function von x in Linearfactoren im Sinne der Congruenz für das Primmodulsystem $(\mathfrak{M})$ benutzt.

EIN SATZ ÜBER DISCRIMINANTEN-FORMEN.

VON

L. KRONECKER.

Crelle, Journal für die reine und angewandte Mathematik. Bd. 100. S. 79—82.

EIN SATZ ÜBER DISCRIMINANTEN-FORMEN.

In einer Abhandlung, welche im 19. Bande des *Liouville*'schen Journals (1854) abgedruckt ist[1]), habe ich den Satz bewiesen, dass derjenige Factor von $x^n - 1$, welcher nur für die *primitiven* n^{ten} Wurzeln der Einheit gleich Null wird, irreductibel ist, und zwar auch dann, wenn eine Wurzel einer ganzzahligen Gleichung adjungirt wird, deren Discriminante zu n relativ prim ist. Dieser Satz ist aber in einem viel allgemeineren enthalten, dessen Erkenntniss ich jenen Principien verdanke, welche ich in den „Grundzügen einer arithmetischen Theorie der algebraischen Grössen" im 92. Bande dieses Journals entwickelt habe[2]).

§ 1.

Es sei $F(x)$ eine ganze Function n^{ten} Grades von x; der Coefficient von x^n sei gleich Eins, und die übrigen Coefficienten seien ganze Grössen eines beliebigen Rationalitätsbereichs, dessen Elemente aus unabhängigen Variabeln und ganzen algebraischen Functionen derselben bestehen. Der Rationalitätsbereich kann hiernach auch ein *Gattungs*bereich sein. Sind nun $\xi_1, \xi_2, \ldots \xi_n$ die Wurzeln der Gleichung $F(x) = 0$, so stellt der Ausdruck:

$$u_1\xi_{r_1} + u_2\xi_{r_2} + \cdots + u_n\xi_{r_n}$$

die verschiedenen Wurzeln der zur Gleichung $F(x) = 0$ zugehörigen *Galois*'schen Gleichung dar, wenn die Grössen u *Unbestimmte* und $(r_1, r_2, \ldots r_n)$ die ver-

[1]) Mémoire sur les facteurs irréductibles de l'expression $x^n - 1$. Band I, S. 75—92 dieser Ausgabe von *L. Kronecker*'s Werken. H.

[2]) Band II. S. 237—387 dieser Ausgabe. H.

schiedenen Permutationen derjenigen Gattung bedeuten, durch welche die *Classe* der Gleichung $F(x) = 0$ charakterisirt wird*).

Dies vorausgeschickt, besteht offenbar die Congruenz:

$$(A.) \qquad \prod_{(r,r')}(\xi_{r_1} - \xi_{r'_1}) \equiv 0 \quad \left(\text{mod. } \prod_{(r,r')}(u_1(\xi_{r_1} - \xi_{r'_1}) + u_2(\xi_{r_2} - \xi_{r'_2}) + \cdots + u_m(\xi_{r_m} - \xi_{r'_m}))\right),$$

wo sich die Producte auf alle Verbindungen je zweier Permutationen $(r_1, r_2, \ldots r_n)$, $(r'_1, r'_2, \ldots r'_n)$ beziehen. Der Modul dieser Congruenz ist aber nichts Anderes als die Discriminante der *Galois*'schen Gleichung und also nach § 9 meiner eben citirten Abhandlung durch die „Discriminantenform" der *Galois*'schen *Gattung* theilbar. Diese ist aber wiederum, gemäss dem a. a. O. bewiesenen Satze, durch die Discriminantenform *jeder* Gattung von Functionen der Wurzeln $\xi_1, \xi_2, \ldots \xi_n$ theilbar. Es ist daher jede solche Discriminantenform in dem Producte:

$$\prod_{(r,r')}(\xi_{r_1} - \xi_{r'_1})$$

enthalten, welches selbst wiederum in einer Potenz der Discriminante von $F(x)$ als Theiler enthalten ist.

Hieraus ergiebt sich der Satz, welcher entwickelt werden sollte, nämlich:

> die Discriminantenform einer jeden aus den verschiedenen Wurzeln einer Gleichung zu bildenden Gattung ist in einer Potenz der Discriminante der Gleichung selbst enthalten,

und hierbei kann, wie unmittelbar zu sehen ist, die Voraussetzung der Irreductibilität der Gleichung fallen gelassen werden.

*) Vgl. § 12 S. 36 meiner citirten Abhandlung im 92. Bande dieses Journals[1]).

[1]) Band II S. 286—287 dieser Ausgabe. H.

Da ferner an Stelle der Gleichung $F(x) = 0$ auch die „Fundamentalgleichung" der durch ξ_1 bestimmten Gattung genommen werden kann, deren Discriminante Theiler einer Potenz der Discriminantenform der Gattung (ξ_1) ist*), so ergiebt sich der Satz auch in folgender Fassung:

> die Discriminantenform einer Gattung (ξ_1) kann zu einer hinreichend hohen Potenz erhoben werden, damit sie durch die Discriminantenform einer jeden aus den verschiedenen *Conjugirten* von ξ_1 zu bildenden Gattung theilbar werde.

In dieser Fassung ist der Satz übrigens auch mit Hülfe von Determinantensätzen herzuleiten, da die Discriminantenform eben nur das Quadrat einer Determinante ist, welche nach § 25 meiner mehrfach citirten Abhandlung ausser den Reihen conjugirter algebraischer Grössen noch Reihen von *Unbestimmten* enthält.

§ 2.

Bedeutet $G(y)$ eine irreductible ganze Function m^{ten} Grades und desselben Bereichs wie $F(x)$, ist ferner der Coefficient von y^m gleich Eins, und sind endlich $\eta_1, \eta_2, \ldots \eta_m$ die Wurzeln der Gleichung $G(y) = 0$, so kann die eine der beiden (im angenommenen Rationalitätsbereich) irreductibeln Gleichungen nur dann unter Adjunction einer Wurzel der anderen reductibel werden, wenn eine gewisse Gattung von rationalen Functionen der Wurzeln ξ mit einer Gattung von rationalen Functionen der Wurzeln η übereinstimmt. Nach dem obigen Satze muss also *die Discriminantenform dieser Gattung gemeinsamer Theiler der beiden Discriminanten von* $F(x)$ *und* $G(y)$ sein.

Nimmt man $F(x) = \frac{x^{p^\nu} - 1}{x^{p^{\nu-1}} - 1}$, wo p eine Primzahl und ν irgend eine ganze Zahl bedeutet, so ist $F(x)$ im absoluten Rationalitätsbereich der natürlichen ganzen Zahlen irreductibel. Denn für jede ganze ganzzahlige Function $f(x)$ findet die Congruenz:

*) Vgl. § 25 der Grundzüge einer arithmetischen Theorie der algebraischen Grössen.

$$f(x)^{p^\nu} \equiv f(x^{p^\nu}) \equiv f(1) \quad (\text{modd. } p,\ x^{p^\nu} - 1)$$

statt, und es wird also, wenn $f(x)$ irgend ein Divisor von $x^{p^\nu} - 1$ ist:

$$f(1) \equiv 0 \quad (\text{modd. } p,\ f(x)),$$

während, wenn $F(x) = f(x)\varphi(x)$, also $F(1) = p = f(1)\varphi(1)$ wäre, einer der beiden Factoren, z. B. $f(1)$, gleich Eins sein müsste.

Ferner ist die Discriminante jeder aus den Wurzeln von $F(x) = 0$ gebildeten Gattung durch p theilbar; denn die Differenz von zwei Horizontalreihen der Determinante, deren Quadrat eben die Discriminante ist, enthält offenbar $1 - x$ als Theiler, und die Discriminante, welche eine ganze Zahl ist, wird daher *modulis* $(1 - x,\ F(x))$, also auch *modulis* $(1 - x,\ F(1))$, also endlich auch *modulo* p, congruent Null.

Hiernach kann $F(x)$ nur dann unter Adjunction einer Wurzel der Gleichung $G(y) = 0$ reductibel werden, wenn die Discriminante von $G(y)$ durch p theilbar ist, und hieraus folgt unmittelbar auch jener Satz, welcher oben in der Einleitung citirt worden ist.

Ich bemerke noch, dass man an Stelle der Function $F(x)$, welche für alle primitiven p^ν-ten Wurzeln der Einheit verschwindet, überhaupt eine ganze Function von der Form:

$$F(x) = (x - 1)^n + p\,\Phi(x)$$

nehmen kann, wo $\Phi(x)$ eine ganze ganzzahlige Function $(n - 1)$-ten Grades bedeutet. Es gilt auch dann noch der Satz, dass jeder Divisor $f(x)$ von $F(x)$ für $x = 1$ *modulis* p, $f(x)$ congruent Null sein muss. Denn $F(x)$ ist *modulo* p ein Divisor von $x^{p^\nu} - 1$, wenn ν so gewählt wird, dass $p^\nu \geq n$ ist; es wird also, wie oben:

$$f(x)^{p^\nu} \equiv f(x^{p^\nu}) \equiv f(1) \quad (\text{modd. } p,\ F(x)), \quad \text{also auch} \quad (\text{modd. } p,\ f(x))$$

und daher:

$$f(1) \equiv 0 \quad (\text{modd. } p,\ f(x)).$$

Hieraus folgt unmittelbar, dass $F(x)$ irreductibel ist, wenn $\Phi(1)$ nicht $\equiv 0$ (mod. p) ist.

Dieses Resultat findet sich schon in dem *Schoenemann*'schen Aufsatze im 32. Bande dieses Journals (§ 61, S. 100[1]) und ist dort auch auf ganz ähnliche Weise hergeleitet. Später hat *Eisenstein* im 39. Bande dieses Journals S. 167 denselben Satz in derselben Art bewiesen[2]), und in manchen Reproductionen wird der Satz irrthümlicher Weise *Eisenstein* zugeschrieben. In einer Notiz im 40. Bande dieses Journals S. 188 hat *Schoenemann* selbst schon auf seine Priorität in der angegebenen Beziehung aufmerksam gemacht; doch findet sich darin (wohl nur in Folge von Druckfehlern) der § 6 seiner Abhandlung im 31. Bande an Stelle des § 61 seiner Abhandlung im 32. Bande citirt.

[1]) *Schönemann*, Grundzüge einer allgemeinen Theorie der höheren Congruenzen, deren Modul eine reelle Primzahl ist; Crelle's Journal Bd. 31, S. 269—325, Bd. 32, S. 93—105. H.

[2]) *G. Eisenstein*, Ueber die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt; Crelle's Journal Bd. 39, S. 160—179, 224—287. H.

ÜBER DEN ZAHLBEGRIFF.

VON

L. KRONECKER.

Crelle, Journal für die reine und angewandte Mathematik. Band 101, S. 337—355.

Philosophische Aufsätze, Eduard Zeller zu seinem fünfzigjährigen Doctor-Jubiläum gewidmet. Leipzig 1887. No. VIII. S. 261—274.

ÜBER DEN ZAHLBEGRIFF*).

Auf dem freien Plane philosophischer Vorarbeit, aus welchem man in die eingehegten Gebiete der verschiedenen Wissenschaften gelangt, sind auch die Begriffe der Zahl, des Raumes und der Zeit zu entwickeln, von welchen in der Mathematik Gebrauch gemacht wird. Und es erscheint zweckmässig, die Entwickelung dort so weit zu führen, dass die Begriffe schon mit ihren Grundeigenschaften ausgestattet sind, wenn die specialwissenschaftliche Behandlung beginnt.

So soll dies hier in Beziehung auf den Zahlbegriff geschehen, den einfachsten jener drei Begriffe, dessen dominirende Stellung *Jacobi* in einem seiner Briefe an *Alexander v. Humboldt* sehr schön hervorgehoben hat**).

„Ein Alter“ — so beginnt einer dieser Briefe — „vergleicht die Mathematiker mit den Lotophagen. Wer einmal, sagt er, die Süssigkeit der mathematischen Ideen gekostet, kann nicht mehr davon ablassen. Schreiben Sie also meinen vorigen Brief***) der Raserei zu, in welche jene Lotosfresser versinken, wenn sie den Cultus jener Ideen vernachlässigt oder sie nur ihrer

*) Dieser Aufsatz ist durch theilweise Umarbeitung und Erweiterung desjenigen entstanden, welcher in den Herrn *Eduard Zeller* zu seinem fünfzigjährigen Doctor-Jubiläum gewidmeten philosophischen Aufsätzen unter No. VIII abgedruckt ist.

**) Die Briefe haben sich in *G. Lejeune Dirichlet*'s Nachlass vorgefunden.

***) Dieser „vorige Brief“ trägt als Datum „Berlin d. 26. Dez. 1846“ und füllt mit der *Jacobi*'schen kleinen und engen Schrift drei Octavseiten vollständig aus. Auf der

zufälligen Anwendungen wegen geschätzt glauben. Und sagt nicht Aehnliches schon *Schiller* in den Xenien in seinem kleinen Gedicht

Archimedes und der Jüngling.

Zu Archimedes kam ein wissbegieriger Jüngling,
Weihe mich, sprach er zu ihm, ein in die göttliche Kunst,
Die so herrliche Dienste der Sternenkunde geleistet,
Hinter dem Uranos noch einen Planeten entdeckt.
Göttlich nennst Du die Kunst, sie ist's, versetzte der Weise,
Aber sie war es, bevor noch sie den Kosmos erforscht,
Ehe sie herrliche Dienste der Sternenkunde geleistet,
Hinter dem Uranos noch einen Planeten entdeckt.
Was Du im Kosmos erblickst, ist nur der Göttlichen Abglanz,
In der Olympier Schaar thronet die ewige Zahl."

In dieser geistvollen Parodie des *Schiller*'schen Gedichts „Archimedes und der Schüler" bezeichnet *Jacobi* die Stellung des Zahlbegriffs in der gesammten Mathematik echt poetisch aber auch genau zutreffend und ganz ähnlich wie *Gauss* in den Worten: „Die Mathematik sei die Königin der Wissenschaften und die Arithmetik die Königin der Mathematik. Diese lasse sich dann öfter herab, der Astronomie und andern Naturwissenschaften einen Dienst zu erweisen, doch gebühre ihr unter allen Verhältnissen der erste Rang"*).

In der That steht die Arithmetik in ähnlicher Beziehung zu den anderen beiden mathematischen Disciplinen, der Geometrie und Mechanik, wie die gesammte Mathematik zur Astronomie und den anderen Naturwissenschaften;

ersten Seite schreibt *Jacobi*: „Also das möchten Sie wissen, welche Gedankenentwickelung vorhergehen musste, damit 1846 *Leverrier* den transuranischen Planeten ausrechnen konnte?" Und auf der dritten Seite: „Unter diesen Umständen ist es also wirklich etwas Ausserordentliches, wenn *Leverrier* bei seiner Rechenfertigkeit die mathematische Umsicht hat, die erforderlich ist, um auf geschickte Art sich an ein weitläufiges gänzlich neues Problem zu wagen. Aber die Arbeit des Menschengeistes kann man nach der dazu nöthigen homöopathischen Dosis nicht ermessen."

*) Vgl. „*Gauss* zum Gedächtniss" von *W. Sartorius v. Waltershausen*, Leipzig 1856, S. 79. In derselben Schrift wird auf S. 97: „*Ὁ θεὸς ἀριθμητίζει*" als ein Ausspruch von *Gauss* angeführt, welcher als solcher durch einen in *G. Lejeune Dirichlet*'s Nachlass vorgefundenen, von *Gauss*' Arzte, *Baum*, an *Humboldt* gerichteten Briefe beglaubigt ist.

auch die Arithmetik erweist der Geometrie und Mechanik mannigfache Dienste und empfängt dagegen von ihren Schwester-Disciplinen eine Fülle von Anregungen. Dabei ist aber das Wort „Arithmetik" nicht in dem üblichen beschränkten Sinne zu verstehen, sondern es sind alle mathematischen Disciplinen mit Ausnahme der Geometrie und Mechanik, also namentlich die Algebra und Analysis, mit darunter zu begreifen. Und ich glaube auch, dass es dereinst gelingen wird, den gesammten Inhalt aller dieser mathematischen Disciplinen zu „arithmetisiren", d. h. einzig und allein auf den im engsten Sinne genommenen Zahlbegriff zu gründen, also die Modificationen und Erweiterungen dieses Begriffs*) wieder abzustreifen, welche zumeist durch die Anwendungen auf die Geometrie und Mechanik veranlasst worden sind. Der principielle Unterschied zwischen der Geometrie und Mechanik einerseits und zwischen den übrigen hier unter der Bezeichnung „Arithmetik" zusammengefassten mathematischen Disciplinen andererseits besteht nach *Gauss* darin, dass der Gegenstand der letzteren, die Zahl, *bloss* unseres Geistes Product ist, während der Raum ebenso wie die Zeit auch *ausser* unserem Geiste eine *Realität* hat, der wir a priori ihre Gesetze nicht vollständig vorschreiben können**).

§ 1.

Definition des Zahlbegriffs.

Den naturgemässen Ausgangspunkt für die Entwickelung des Zahlbegriffs finde ich in den *Ordnungszahlen*. In diesen besitzen wir einen Vor-

*) Ich meine hier namentlich die Hinzunahme der irrationalen sowie der continuirlichen Grössen.

**) Die *Gauss*'schen Worte (in einem Briefe an *Bessel* vom 9. April 1830[1]) lauten: „Nach meiner innigsten Ueberzeugung hat die Raumlehre zu unserm Wissen a priori eine ganz andere Stellung, wie die reine Grössenlehre; es geht unserer Kenntniss von jener durchaus *diejenige* vollständige Ueberzeugung von ihrer Nothwendigkeit (also auch von ihrer absoluten Wahrheit) ab, die der *letztern* eigen ist; wir müssen in Demuth zugeben, dass, wenn die Zahl *bloss* unsers Geistes Product ist, der Raum auch *ausser* unserm Geiste eine *Realität* hat, der wir a priori ihre Gesetze nicht vollständig vorschreiben können." Vgl. Herrn *Ernst Schering*'s Festrede, vorgetragen in der öffentlichen Sitzung der Königlichen Gesellschaft der Wissenschaften zu Göttingen am 30. April 1877, S. 9.

[1]) Briefwechsel zwischen *Gauss* und *Bessel*, Leipzig 1880, S. 497 flgde. H.

rath gewisser, nach einer festen Reihenfolge geordneter Bezeichnungen, welche wir einer Schaar verschiedener und zugleich für uns unterscheidbarer Objecte beilegen können*). *Die Gesammtheit der hierbei verwendeten Bezeichnungen* fassen wir in dem Begriffe der „Anzahl der Objecte", aus denen die Schaar besteht, zusammen, und wir knüpfen den Ausdruck für diesen Begriff unzweideutig an die *letzte* der verwendeten Bezeichnungen an, da deren Aufeinanderfolge fest bestimmt ist. So kann z. B. in der Schaar der Buchstaben (a, b, c, d, e) dem Buchstaben a die Bezeichnung als „erster", dem Buchstaben b die Bezeichnung als „zweiter" u. s. f. und endlich dem Buchstaben e die Bezeichnung als „fünfter" beigelegt werden. Die Gesammtheit der dabei verwendeten Ordnungszahlen oder die „Anzahl" der Buchstaben a, b, c, d, e kann demgemäss in Anknüpfung an die letzte der verwendeten Ordnungszahlen durch die Zahl „Fünf" bezeichnet werden**).

*) Die Objecte können in gewissem Sinne einander gleich und nur räumlich, zeitlich oder gedanklich unterscheidbar sein, wie z. B. zwei gleiche Längen oder zwei gleiche Zeittheile.

**) Der Vorrath von Bezeichnungen, den wir in den Ordnungszahlen besitzen, ist deshalb immer ausreichend, weil es nicht sowohl ein wirklicher als vielmehr ein ideeller Vorrath ist. In den Gesetzen der *Bildung* unserer Wort- und Zifferbezeichnung der Zahlen besitzen wir recht eigentlich das „Vermögen", jeden Anspruch zu befriedigen. Freilich nur in *der* Weise, dass in dem Ausdrucke einer Zahl gewisse Bezeichnungen beliebig vielfach wiederholt werden. Sind aber Wiederholungen gestattet, so genügt schon ein einziges Zeichen, um jede Zahl auszudrücken, nämlich so, dass das eine Zeichen so oft wiederholt wird, als die Zahl angiebt. Indessen wäre eine solche primitive Darstellungsweise mittels eines einzigen Zeichens ganz unübersichtlich, und die andere ebenso primitive Darstellungsweise durch lauter verschiedene Zeichen wäre offenbar ganz unthunlich. Man ist deshalb bei den Wortbezeichnungen der Zahlen wohl darauf ausgegangen, mit Hülfe möglichst wenig specifisch verschiedener Stammworte möglichst viele Zahlen auszudrücken, und dies ist dadurch gelungen, dass man das Schema der Bezeichnungen wie eine Tabelle mit zweifachem Eingang einrichtete. So kann man durch Einzeichnung von Punkten in die 45 Felder einer durch fünf Colonnen und neun Zeilen gebildeten Tabelle alle Zahlen bis 99 999 genau so darstellen, wie es durch die griechische Wortbezeichnung geschieht. Werden dabei in die Colonne I die Einer, in die Colonne II die Zehner, in die Colonne III die Hunderter, in die Colonne IV die Tausender und in die Colonne V die Zehntausender eingezeichnet, so wird z. B. die Zahl 32 456 durch fünf Punkte dargestellt, welche beziehungsweise

in den Zeilen 3, 2, 4, 5, 6
und in den Colonnen V, IV, III, II, I

Man kann aus den Ordnungszahlen selbst eine Schaar von Objecten bilden. Für diejenige Schaar, welche aus einer bestimmten (n^{ten}) Ordnungszahl und aus allen vorhergehenden Ordnungszahlen besteht, wird die „Anzahl" gemäss der oben gegebenen Definition durch die der n^{ten} Ordnungszahl entsprechende „Cardinalzahl" n ausgedrückt, und es sind diese Cardinalzahlen, welche auch schlechthin als „Zahlen" bezeichnet werden. Eine Zahl m heisst „kleiner" als eine andere Zahl n, wenn die zu m gehörige Ordnungszahl der zu n gehörigen vorangeht. Die sogenannte natürliche Reihenfolge der Zahlen ist nichts Anderes als die Reihenfolge der entsprechenden Ordnungszahlen.

§ 2.

Die Unabhängigkeit der Zahl von der beim Zählen befolgten Anordnung.

Wenn man eine Schaar von Objecten „zählt", d. h. wenn man die Ordnungszahlen, ihrer Reihenfolge nach, den einzelnen Objecten als Bezeichnungen beilegt, so giebt man damit den Objecten selbst eine bestimmte Anordnung. Wenn nun diese Anordnung der Objecte beibehalten, aber eine neue Reihenfolge der als Bezeichnungen verwendeten Ordnungszahlen (durch irgend eine Permutation derselben) festgesetzt und alsdann dem ersten Objecte die in der neuen Reihenfolge erste Ordnungszahl, dem zweiten Objecte die zweite Ordnungszahl, und so der Reihe nach jedem folgenden Objecte die folgende Ordnungszahl als Bezeichnung beigelegt wird, so erhalten damit die Objecte wiederum eine durch die ihnen zugetheilten Ordnungszahlen bestimmte, von der früheren verschiedene Anordnung, und sie werden

stehen. Die griechische Wortbezeichnung τρισμύριοι δισχίλιοι τετρακόσιοι πεντήκοντα ἕξ ergiebt sich aus einer solchen Tabelle unmittelbar, indem man aus der Zeilenbezeichnung den Anfang und aus der Colonnenbezeichnung die Endung jedes einzelnen der fünf Zahlwörter entnimmt. Demnach ist für den ersten Punkt, welcher in der Zeile 3 (τρεῖς) und in der Colonne V (μύριοι) steht, das Zahlwort τρισμύριοι zu bilden, für den zweiten Punkt, welcher in der Zeile 2 (δύο) und in der Colonne IV (χίλιοι) steht, das Zahlwort δισχίλιοι u. s. f., und für den fünften Punkt, welcher in der Zeile 6 (ἕξ) und in der Colonne I steht, bleibt das Zahlwort ἕξ selbst ohne Zusatz einer Endung. Die griechische Zahlwörterbildung ermöglicht es also, mit Hülfe von nur 13 verschiedenen Bezeichnungen, nämlich neun Anfangs- und vier Endungsbezeichnungen, alle Zahlen bis 99 999 deutlich unterscheidbar auszudrücken.

also in einer anderen Anordnung „gezählt“*). Dabei bleibt aber die „Gesammtheit“ der als Bezeichnungen verwendeten Ordnungszahlen, welche nach der obigen Definition den Begriff der „Anzahl der Objecte“ ergiebt, ungeändert, und diese Anzahl, d. h. das *Resultat* des Zählens, ist demnach von der beim Zählen befolgten oder durch das Zählen gegebenen Anordnung unabhängig. Die „Anzahl“ der Objecte einer Schaar ist also eine Eigenschaft der Schaar als solcher, d. h. der unabhängig von irgend einer bestimmten Anordnung gedachten Gesammtheit der Objecte.

Fasst man irgend welche Elemente, die mit den Buchstaben $a, b, c, d, \ldots$ bezeichnet werden mögen, gedanklich zu einem System zusammen, aber so, dass auch die Reihenfolge der Elemente dabei fixirt wird, so sind z. B. die beiden Systeme (a, b, c) und (c, a, b) von einander verschieden. Und in der That sind auch, wenn man für a, b, c irgend welche von einander verschiedene Zahlen nimmt und dann einen Punkt im Raume, dessen drei rechtwinklige Coordinaten durch die Werthe $x = a$, $y = b$, $z = c$ bestimmt sind, durch das System (a, b, c) bezeichnet, die zwei Punkte (a, b, c) und (c, a, b) von einander verschieden. Wenn nun aber irgend zwei Systeme $(a, b, c, d, \ldots)$, $(a', b', c', d', \ldots)$ *„äquivalent“* genannt werden, sobald es möglich ist, das eine in das andere dadurch zu transformiren, dass man der Reihe nach jedes Element des ersten Systems durch je eines des zweiten Systems ersetzt, so besteht die nothwendige und hinreichende Bedingung für die Aequivalenz zweier Systeme in der Gleichheit der Anzahl ihrer Elemente, und die Anzahl der Elemente eines Systems $(a, b, c, d, \ldots)$ charakterisirt sich hiernach als die einzige *„Invariante“* aller untereinander äquivalenten Systeme**).

*) Für die Darlegung der Möglichkeit, Objecte in verschiedenen Anordnungen zu zählen, ist hier absichtlich nicht das Permutiren der Objecte selbst, sondern nur das der Zahlbezeichnungen benutzt worden. Es bedurfte auf diese Weise keiner weiteren Voraussetzung über die Objecte, als jener im § 1, wonach sie „unterscheidbar“ sind.

**) Hierdurch wird, glaube ich, der Inhalt des Satzes näher präcisirt, mit welchem Herr *Lipschitz* sein Lehrbuch der Analysis beginnt. Dieser Satz lautet: „Wenn man bei der Betrachtung getrennter Dinge von den Merkmalen absieht, durch welche sich die Dinge unterscheiden, so bleibt der Begriff der *Anzahl* der betrachteten Dinge zurück.“

§ 3.

Die Addition der Zahlen.

Man kann die Zahlen selbst als Objecte des Zählens nehmen. Man kann also z. B. von der Zahl $n_1 + 1$ an um n_2 weiter zählen, d. h. genau so viele von den auf die Zahl n_1 zunächst folgenden Zahlen zu einer Schaar zusammenfassen, dass deren Anzahl n_2 beträgt. Dieses „weiter Zählen“ heisst: *„zur Zahl n_1 die Zahl n_2 addiren“*, und diejenige Zahl s, zu welcher man bei jenem weiter Zählen gelangt, heisst das „Resultat der Addition“ oder die „Summe von n_1 und n_2“ und wird durch $n_1 + n_2$ dargestellt. Zu eben demselben Resultat s gelangt man aber auch, wenn man zur Zahl n_2 die Zahl n_1 addirt, d. h. wenn man von der Zahl $n_2 + 1$ anfangend um n_1 weiter zählt, und es ist daher: $n_1 + n_2 = n_2 + n_1$. Ebenso ist allgemein: $n_1 + n_2 + n_3 + \cdots + n_r = n_\alpha + n_\beta + n_\gamma + \cdots + n_\varrho$, wenn $\alpha, \beta, \gamma, \ldots \varrho$ die Zahlen $1, 2, 3, \ldots r$ in irgend einer Anordnung bedeuten. Denn, wenn man die ganze Schaar von Systemen zweier Zahlen (h, k) bildet, welche entsteht, indem man nach einander:

$$\begin{aligned}
&h = 1 \quad \text{und} \quad k = 1, 2, \ldots n_1,\\
&h = 2 \quad \text{und} \quad k = 1, 2, \ldots n_2,\\
&h = 3 \quad \text{und} \quad k = 1, 2, \ldots n_3,\\
&\ldots\ldots\ldots\ldots\\
&\ldots\ldots\ldots\ldots\\
&h = r \quad \text{und} \quad k = 1, 2, \ldots n_r
\end{aligned}$$

setzt, so ergiebt sich die Zahl: $n_1 + n_2 + n_3 + \cdots + n_r$, als Anzahl der Systeme der Schaar, sobald man sie in der Reihenfolge zählt, in welcher sie hier gebildet worden sind. Ordnet man sie aber dergestalt, dass diejenigen nach einander folgen, in denen:

$$\begin{aligned}
&h = \alpha \quad \text{und} \quad k = 1, 2, \ldots n_\alpha,\\
&h = \beta \quad \text{und} \quad k = 1, 2, \ldots n_\beta,\\
&h = \gamma \quad \text{und} \quad k = 1, 2, \ldots n_\gamma,\\
&\ldots\ldots\ldots\ldots\\
&\ldots\ldots\ldots\ldots\\
&h = \varrho \quad \text{und} \quad k = 1, 2, \ldots n_\varrho
\end{aligned}$$

ist, so ergiebt sich die Zahl $n_\alpha + n_\beta + n_\gamma + \cdots + n_\varrho$, als Anzahl der Systeme der Schaar, und dieselbe Anzahl wird also einerseits durch die Summe: $n_1 + n_2 + n_3 + \cdots + n_r$, andererseits durch die Summe: $n_\alpha + n_\beta + n_\gamma + \cdots + n_\varrho$ dargestellt.

§ 4.

Die Multiplication der Zahlen.

Sind die einzelnen Summanden $n_1, n_2, n_3, \ldots n_r$ sämmtlich gleich einer und derselben Zahl n, so bezeichnet man die Addition als „Multiplication der Zahl n mit dem Multiplicator r“ und setzt:

$$n_1 + n_2 + n_3 + \cdots + n_r = rn.$$

Das Resultat der so definirten Multiplication bezeichnet man als das Product der Zahlen r und n. Man erhält aber genau dasselbe Resultat, wenn man die Zahl r mit dem Multiplicator n multiplicirt, und es ist überhaupt das Product beliebig vieler Zahlen $n_1 n_2 n_3 \cdots n_r$ unabhängig von der Reihenfolge, in welcher die Multiplicationen nach einander ausgeführt werden. Denn wenn man sich die sämmtlichen Systeme von r Zahlen $(h_1, h_2, h_3, \ldots h_r)$ gebildet denkt, welche entstehen, indem man

für h_1 alle Werthe $1, 2, 3, \ldots n_1$,
für h_2 alle Werthe $1, 2, 3, \ldots n_2$,
für h_3 alle Werthe $1, 2, 3, \ldots n_3$,
. . . . . .
. . . . . .
für h_r alle Werthe $1, 2, 3, \ldots n_r$,

setzt, so können diese Systeme nach der Grösse der Werthe von

$$h_r + h_{r-1} g + h_{r-2} g^2 + \cdots + h_1 g^{r-1}$$

geordnet werden, wenn g eine Zahl bedeutet, die grösser als jede der Zahlen

$n_1, n_2, n_3, \ldots n_r$ ist. Die Systeme folgen dann so auf einander, wie sie der Grösse nach auf einander folgen würden, wenn $h_1 h_2 h_3 \cdots h_r$ eine Zahl mit den *Ziffern* $h_1, h_2, h_3, \ldots h_r$ in dem Zahlensysteme mit der Grundzahl g darstellte. Das Princip einer solchen Anordnung ist übrigens kein anderes als das lexikographische für den Fall, dass an die Stelle der Zahlen $1, 2, 3, \ldots$ der Reihe nach die Buchstaben eines Alphabets treten.

Die verschiedenen Abtheilungen der Systeme $(h_1, h_2, h_3, \ldots h_r)$, welche durch die verschiedenen Werthe von h_1 charakterisirt werden, und deren Anzahl n_1 ist, folgen einander bei der angegebenen Anordnung nach der Grösse der Werthe von h_1; innerhalb jeder Abtheilung folgen die n_2 verschiedenen, durch die Werthe von h_2 charakterisirten Unterabtheilungen wiederum einander nach der Grösse *dieser* Werthe u. s. f. Bezeichnet man die Anzahl derjenigen Systeme, in denen $h_1 = 1$ ist, mit s_1, so ist s_1 auch die Anzahl der Systeme in *jeder* der n_1 Abtheilungen, welche durch die Werthe: $h_1 = 1, 2, 3, \ldots n_1$ charakterisirt werden. Die Gesammtanzahl aller Systeme wird hiernach durch das Product $n_1 s_1$ ausgedrückt. Bezeichnet man nun ferner die Anzahl derjenigen Systeme, in denen $h_1 = 1$ und $h_2 = 1$ ist, mit s_2, so ist s_2 auch die Anzahl der Systeme in jeder der n_2 Unterabtheilungen, welche bei Festhaltung des Werthes $h_1 = 1$ durch die n_2 Werthe: $h_2 = 1, 2, 3, \ldots n_2$ charakterisirt werden. Die mit s_1 bezeichnete Anzahl aller Systeme der Abtheilung, in welcher $h_1 = 1$ ist, wird also durch das Product $n_2 s_2$ ausgedrückt, und die Anzahl aller Systeme überhaupt wird gleich: $n_1 n_2 s_2$. Fährt man auf diese Weise fort, so erhält man das Product: $n_1 n_2 n_3 \cdots n_r$ als Ausdruck für die Anzahl der sämmtlichen Systeme $(h_1, h_2, h_3, \ldots h_r)$.

Bedeuten nun, wie oben, $\alpha, \beta, \gamma, \ldots \varrho$ die Zahlen $1, 2, 3, \ldots r$ in irgend einer andern Anordnung, und ordnet man die sämmtlichen Systeme $(h_1, h_2, h_3, \ldots h_r)$ so, wie sie der Grösse nach auf einander folgen würden, wenn $h_\alpha h_\beta h_\gamma \cdots h_\varrho$ eine Zahl mit den Ziffern $h_\alpha, h_\beta, h_\gamma, \ldots h_\varrho$ in dem Zahlensysteme mit der Grundzahl g darstellte, so erhält man bei dem auseinandergesetzten Verfahren das Product: $n_\alpha n_\beta n_\gamma \cdots n_\varrho$ als Ausdruck für die Anzahl der sämmtlichen Systeme $(h_1, h_2, h_3, \ldots h_r)$, und es muss also in der That:

$$n_1 n_2 n_3 \cdots n_r = n_\alpha n_\beta n_\gamma \cdots n_\varrho$$

sein. Das Product beliebig vieler Zahlen ist demnach unabhängig von der Reihenfolge der Factoren, d. h. von der Reihenfolge, in welcher die Multiplicationen nach einander ausgeführt werden.

§ 5.

Die Buchstabenrechnung.

Die Gesetze der Addition und der Multiplication der Zahlen sind hiermit aus den Definitionen vollständig entwickelt. Dieselben Gesetze mussten für die sogenannte Buchstabenrechnung als maassgebend angenommen werden, sobald man anfing, die Buchstaben zur Bezeichnung von Zahlen zu verwenden, deren Bestimmung vorbehalten bleiben kann oder soll. Aber mit der *principiellen* Einführung der „Unbestimmten" (indeterminatae), welche von *Gauss* herrührt, hat sich die specielle Theorie der ganzen Zahlen zu der allgemeinen arithmetischen Theorie der ganzen ganzzahligen Functionen von Unbestimmten erweitert. Diese allgemeine Theorie gestattet alle der eigentlichen Arithmetik fremden Begriffe, den der negativen, der gebrochenen, der reellen und der imaginären algebraischen Zahlen, auszuscheiden.

I. Der Begriff der *negativen* Zahlen kann vermieden werden, indem in den Formeln der Factor -1 durch eine Unbestimmte x und das Gleichheitszeichen durch das *Gauss*'sche Congruenzzeichen *modulo* $(x+1)$ ersetzt wird. So wird die Gleichung:

$$7 - 9 = 3 - 5$$

in die Congruenz:

$$7 + 9x \equiv 3 + 5x \pmod{x+1}$$

transformirt; sie gewinnt dadurch auch an Inhalt, da die Congruenz für jede positive ganze Zahl x eine Bedeutung hat, nämlich die, dass $7+9x$ bei der Division durch $x+1$ denselben Rest lässt wie $3+5x$, und andererseits geht diese Congruenz unmittelbar in die Gleichung über, sobald man

x nicht mehr als Unbestimmte, sondern als eine durch die Gleichung $x+1=0$ definirte „Grösse" auffasst und also die „negative Einheit" einführt. Dass übrigens die Bedeutung der Formel: $7-9=3-5$ selbst einer näheren Darlegung bedarf, und dass dabei „eigentlich ein neuer Gebrauch vom Gleichheitszeichen" gemacht wird, findet man in dem Lehrbuch des Herrn Dr. *Hermann Schubert* klar auseinandergesetzt*).

II. Der Begriff der *gebrochenen* Zahlen ist zu vermeiden, indem man in den Formeln den Factor $\frac{1}{m}$ durch eine Unbestimmte x_m und das Gleichheitszeichen durch das *Gauss*'sche Congruenzzeichen *modulo* $(mx_m - 1)$ ersetzt. Die drei Bruchrechnungsregeln, nämlich die der Addition:

$$\frac{a}{m} + \frac{b}{n} = \frac{an+bm}{mn},$$

die der Multiplication:

$$\frac{a}{m} \cdot \frac{b}{n} = \frac{ab}{mn},$$

und die der Division:

$$\frac{a}{m} : \frac{b}{n} = \frac{an}{bm},$$

werden alsdann vollständig durch die drei entsprechenden Congruenzen:

(1.) $ax_m + bx_n \equiv (an+bm)x_{mn} \pmod{mx_m - 1,\ nx_n - 1,\ mnx_{mn} - 1}$,

(2.) $ax_m \cdot bx_n \equiv abx_{mn} \pmod{mx_m - 1,\ nx_n - 1,\ mnx_{mn} - 1}$,

(3.) $ax_m \cdot x_{bx_n} \equiv anx_{bm} \pmod{mx_m - 1,\ nx_n - 1,\ bmx_{bm} - 1,\ bx_n x_{bx_n} - 1}$

begründet. Diese drei Congruenzen selbst resultiren aber aus den drei folgenden Identitäten:

---

*) System der Arithmetik und Algebra, als Leitfaden für den Unterricht in höheren Schulen. Von Dr. *Hermann Schubert*, Oberlehrer an der Gelehrtenschule des Johanneums in Hamburg. Potsdam 1885. Verlag von Aug. Stein. S. 26. Von der im § 5 eben dieses Werkes enthaltenen Entwickelung des „Begriffs der Zahl" ist Manches bei den obigen Auseinandersetzungen benutzt worden.

$$\text{(I.)}\quad \begin{cases} ax_m + bx_n = (an+bm)x_{mn} + anx_{mn}(mx_m - 1) + bmx_{mn}(nx_n - 1) \\ \qquad\qquad - (ax_m + bx_n)(mnx_{mn} - 1), \end{cases}$$

$$\text{(II.)}\quad \begin{cases} ax_m \cdot bx_n = abx_{mn} + abnx_n x_{mn}(mx_m - 1) + abx_{mn}(nx_n - 1) \\ \qquad\qquad - abx_m x_n(mnx_{mn} - 1), \end{cases}$$

$$\text{(III.)}\quad \begin{cases} ax_m \cdot x_{bx_n} = anx_{bm} + anx_{bm}(mx_m - 1) - abmx_m x_{bm} x_{bx_n}(nx_n - 1) \\ \qquad\qquad - ax_m x_{bx_n}(bmx_{bm} - 1) + amnx_m x_{bm}(bx_n x_{bx_n} - 1). \end{cases}$$

Das „Grösser" und „Kleiner" der Brüche kann als durch die Additionsregel gegeben betrachtet werden, indem der durch Addition zweier Brüche entstandene Bruch für grösser als jeder der beiden Summanden erklärt wird. Auf diese Weise wird die Aufeinanderfolge der rationalen Brüche nicht bloss definirt, sondern auch begründet*).

III. Dass die Einführung und Verwendung der *algebraischen* Zahlen überall da entbehrlich ist, wo nicht die Isolirung der unter einander conjugirten erfordert wird, habe ich in einem früheren Aufsatze gezeigt**); dass

*) In der Vorrede zu seinem Werke: „Introduction à la théorie des fonctions d'une variable" sagt Herr *Jules Tannery* S. VIII: „On peut constituer entièrement l'Analyse avec la notion de nombre entier et les notions relatives à l'addition des nombres entiers; il est inutile de faire appel à aucun autre postulat, à aucune autre donnée de l'expérience; . . . . une fraction, du point de vue que j'indique, ne peut pas être regardée comme la réunion de parties égales de l'unité; ces mots „parties de l'unité" n'ont plus de sens; une fraction est un ensemble de deux nombres entiers, rangés dans un ordre déterminé; sur cette nouvelle espèce de nombres, il y a lieu de reprendre les définitions de l'égalité, de l'inégalité et des opérations arithmétiques". Wie dies letztere in der That — wenn auch in anderer Reihenfolge — geschehen kann, ist oben dargelegt worden.

**) „Ein Fundamentalsatz der allgemeinen Arithmetik" Bd. 100, S. 490 dieses Journals. Man vergleiche namentlich den Schluss dieses Aufsatzes a. a. O. S. 510[1]). Dem dort Gesagten ist hinzuzufügen, dass in gewissen Gebieten der Algebra die Verwendung der Moduln und Modulsysteme an Stelle der algebraischen Zahlen nicht nur zulässig, sondern sogar nothwendig ist. So kann die Frage, ob eine irreductible ganzzahlige Function $F(x)$ unter Adjunction einer Wurzel einer irreductibeln ganzzahligen Gleichung $\Phi(y) = 0$ reductibel wird, nur in *der* Form entschieden werden, ob $F(x)$ sich *modulo* $\Phi(y)$ als Product ganzer Functionen von x und y mit rationalen Coefficienten darstellen lässt.

[1]) Band III S. 209—240 dieser Ausgabe. Vgl. besonders S. 240. H.

diese Isolirung selbst aber auch ohne Einführung neuer Begriffe geschehen kann und nur dann, wenn sie so geschieht, das Wesen der Sache klar hervortreten lässt, soll hier in derselben Weise, wie ich es seit zehn Jahren in meinen Universitätsvorlesungen zu thun pflege, dargelegt und damit zugleich jene „genauere Analyse des Begriffs der reellen Wurzeln algebraischer Gleichungen" gegeben werden, welche ich am Schlusse des ersten Theiles der „Grundzüge einer arithmetischen Theorie der algebraischen Grössen" angekündigt habe*).

Ist $f(x)$ eine ganze ganzzahlige Function von x, welche mit ihrer Ableitung $f'(x)$ keinen Theiler gemein hat, so giebt es ganze ganzzahlige Functionen $\varphi(x)$, $\varphi_1(x)$, für welche die Gleichung:

$$\text{(2.)}\qquad \varphi(x)f(x) + \varphi_1(x)f'(x) = D$$

besteht. Hier bedeutet D den absoluten Werth der Discriminante von $f(x)$, also eine positive ganze Zahl. Es sei nun:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

und a_g der absolut grösste der n Coefficienten a_0, a_1, . . . a_{n-1}. Bezeichnet man alsdann den rationalen Bruch $\frac{|a_g| + |a_n|}{|a_n|}$ mit $\mathfrak{r}$, so ist:

$$\left|\frac{f(x)}{a_n} - x^n\right| < (\mathfrak{r} - 1)\frac{|x|^n - 1}{|x| - 1},$$

also für jeden nicht zwischen $-\mathfrak{r}$ und $\mathfrak{r}$ liegenden Werth von x:

$$|f(x) - a_n x^n| < |a_n x^n| \quad \text{und folglich:} \quad \operatorname{sgn} f(x) = \operatorname{sgn} a_n x^n.$$

Demnach kann $f(x)$ nur innerhalb des Intervalles $(-\mathfrak{r}, \mathfrak{r})$ sein Vorzeichen ändern.

*) B. 92, S. 44 dieses Journals.[1])

[1]) Band II S. 296 dieser Ausgabe. H.

Setzt man zur Abkürzung:

$$f(x+\sigma)-f(x)=\sigma f_1(x,\sigma), \quad (f_1(x,\sigma)-f'(x))\varphi_1(x)=\sigma\psi(x,\sigma),$$

so sind $f_1(x,\sigma)$ und $\psi(x,\sigma)$ ganze ganzzahlige Functionen von x und σ, und wenn man unter $\overline{f}_1(x,\sigma)$, $\overline{\varphi}(x)$, $\overline{\varphi}_1(x)$, $\overline{\psi}(x,\sigma)$ beziehungsweise diejenigen Functionen versteht, welche aus $f_1(x,\sigma)$, $\varphi(x)$, $\varphi_1(x)$, $\psi(x,\sigma)$ dadurch hervorgehen, dass man darin die Coefficienten durch ihre absoluten Werthe ersetzt, so bestehen offenbar die Ungleichheiten:

$$|f_1(x,\sigma)|<\overline{f}_1(\mathfrak{r},1), \quad |\varphi(x)|<\overline{\varphi}(\mathfrak{r}), \quad |\varphi_1(x)|<\overline{\varphi}_1(\mathfrak{r}), \quad |\psi(x,\sigma)|<\overline{\psi}(\mathfrak{r},1),$$

sobald der Werth von x zwischen $-\mathfrak{r}$ und $\mathfrak{r}$ und σ zwischen -1 und 1 liegt. Bedeutet nun s eine ganze Zahl, welche den grössten der vier rationalen Werthe:

$$\frac{\overline{f}_1(\mathfrak{r},1)}{D}, \quad \frac{\overline{\varphi}(\mathfrak{r})}{D}, \quad \frac{\overline{\varphi}_1(\mathfrak{r})}{D}, \quad \frac{\overline{\psi}(\mathfrak{r},1)}{D}$$

mindestens um eine Einheit übersteigt, und setzt man dann:

$$\varphi(x)=(s-1)D\theta(x), \quad \varphi_1(x)=(s-1)D\theta_1(x), \quad \psi(x,\sigma)=(s-1)DH(x,\sigma),$$

so geht die Gleichung (𝔄.) in folgende über:

(𝔅.) $$\theta(x)f(x)+\theta_1(x)\cdot\frac{f(x+\sigma)-f(x)}{\sigma}=\sigma H(x,\sigma)+\frac{1}{s-1},$$

und die Werthe der Functionen $\theta(x)$, $\theta_1(x)$, $H(x,\sigma)$ sind für die Werthe von x und σ, welche durch die Ungleichheiten:

$$-\mathfrak{r}<x<\mathfrak{r}, \quad -1<\sigma<1$$

beschränkt sind, absolut kleiner als Eins. Ist σ absolut kleiner als $\frac{1}{s}$, so folgt aus der Gleichung (𝔅.) die Ungleichheit:

$$|f(x)|+\left|\frac{f(x+\sigma)-f(x)}{\sigma}\right|>\frac{1}{s(s-1)},$$

und es besteht daher für je zwei in dem Intervall $(-\mathfrak{r},\mathfrak{r})$ liegende Werthe x', x'', deren Differenz, absolut genommen, kleiner als $\frac{1}{s}$ ist, die Ungleichheit:

(𝔇.) $$|f(x')|+\left|\frac{f(x'')-f(x')}{x''-x'}\right|>\frac{1}{s(s-1)}.$$

Es soll nunmehr gezeigt werden, dass die Function $f(x)$, während x in einem Intervalle von der Grösse $\frac{1}{s}$ bleibt, entweder gar nicht oder nur *ein* Mal ihr Zeichen wechselt, d. h. dass, wenn:

$$x'<x''<x''' \quad \text{und} \quad x'''-x'\leqq\frac{1}{s}$$

ist, nicht:

$$\operatorname{sgn}.f(x')=-\operatorname{sgn}.f(x'')=\operatorname{sgn}.f(x''')$$

sein kann.

Hat der Werth von $f(x)$ am Anfange eines Intervalls, welches nicht grösser als $\frac{1}{s}$ ist und mit (J) bezeichnet werden möge, das entgegengesetzte Vorzeichen desjenigen am Ende des Intervalls, so muss dasselbe auch wenigstens für eines der Theilintervalle der Fall sein, in welche das Intervall (J) getheilt werden kann. Es sei nun r eine beliebige ganze Zahl, und man denke sich das Intervall (J) in rD gleiche Theile getheilt. Alsdann sei (J') ein solches dieser Theilintervalle, in welchem Anfangs- und Endwerth von $f(x)$ entgegengesetztes Zeichen hat. Endlich seien x', x'' irgend zwei in dem Intervalle (J') liegende Werthe von x, wofür:

$$x'<x'', \quad \operatorname{sgn}.f(x')=-\operatorname{sgn}.f(x'')$$

ist. Da nun:

$$f(x'')-f(x')=(x''-x')f_1(x',x''-x')$$

und also:

(𝔇.) $$|f(x'') - f(x')| < (x'' - x')\,\overline{f}_1(\mathfrak{r}, 1) \leqq (x'' - x')\,(s-1)\,D$$

ist, so folgt mit Berücksichtigung der Ungleichheit: $x'' - x' \leqq \frac{1}{rsD}$, dass:

$$|f(x'') - f(x')| < \frac{1}{r},$$

und also, da $f(x')$ und $f(x'')$ entgegengesetzte Vorzeichen haben, auch:

(𝔈.) $$|f(x')| < \frac{1}{r}, \qquad |f(x'')| < \frac{1}{r}$$

sein muss. *In jedem Intervalle von der Grösse* $\frac{1}{s}$, *an dessen Anfangs- und Endpunkt* $f(x)$ *entgegengesetztes Vorzeichen hat, kann also, wenn man eine ganze Zahl* r *beliebig wählt, mindestens ein Intervall von der Grösse* $\frac{1}{rsD}$ *gefunden werden, an dessen Anfangs- und Endpunkt ebenfalls* $f(x)$ *entgegengesetztes Vorzeichen hat, und in welchem alle Werthe von* $f(x)$ *absolut kleiner als* $\frac{1}{r}$ *sind.*

Wenn $f(x)$ am Anfange eines Intervalles, welches nicht grösser als $\frac{1}{s}$ ist, *dasselbe* Vorzeichen hat wie an dessen Endpunkt, so behält $f(x)$ eben dieses Vorzeichen innerhalb des ganzen Intervalles.

Bezeichnet man nämlich das Intervall mit (J^0), seinen Anfangspunkt mit x_0, seinen Endpunkt mit x_4, und nimmt man an, dass für einen zwischen x_0 und x_4 liegenden Werth x_2 die Function $f(x)$ ein anderes Vorzeichen hätte als $f(x_0)$ und $f(x_4)$, so liessen sich auch zwei zu beiden Seiten von x_2 und noch innerhalb des Intervalls (J^0) liegende Werthe x_1 und x_3 durch die Gleichungen:

(𝔉.) $$x_1 = x_2 - \frac{|f(x_2)|}{(s-1)\,D}, \qquad x_3 = x_2 + \frac{|f(x_2)|}{(s-1)\,D}$$

bestimmen, für welche:

$$\text{sgn.}\, f(x_0) = -\,\text{sgn.}\, f(x_1) = \text{sgn.}\, f(x_4) = -\,\text{sgn.}\, f(x_3)$$

wäre. Denn, dass erstens die Werthe x_1 und x_3 noch innerhalb des Intervalles (J^0) liegen, d. h. dass die Ungleichheiten:

$$x_2 - x_0 > \frac{|f(x_2)|}{(s-1)\,D}, \qquad x_4 - x_2 > \frac{|f(x_2)|}{(s-1)\,D}$$

bestehen, erschliesst man aus den Ungleichheiten:

$$|f(x_2) - f(x_0)| < (x_2 - x_0)\,(s-1)\,D, \quad |f(x_4) - f(x_2)| < (x_4 - x_2)\,(s-1)\,D,$$

welche aus der obigen Ungleichheit (𝔇.) hervorgehen, indem man überdies berücksichtigt, dass der Voraussetzung nach:

$$\text{sgn.}\, f(x_2) = -\,\text{sgn.}\, f(x_0) = -\,\text{sgn.}\, f(x_4)$$

ist. Es ist nun zweitens gemäss der obigen Ungleichheit (𝔇.):

$$|f(x_2) - f(x_1)| < (x_2 - x_1)\,(s-1)\,D, \quad |f(x_3) - f(x_2)| < (x_3 - x_2)\,(s-1)\,D,$$

also in Folge der Gleichungen (𝔉.):

$$|f(x_2) - f(x_1)| < |f(x_2)|, \quad |f(x_3) - f(x_2)| < |f(x_2)|,$$

und diese Ungleichheiten erfordern, dass sowohl $f(x_1)$ als auch $f(x_3)$ dasselbe Vorzeichen habe wie $f(x_2)$, also das entgegengesetzte der Functionswerthe $f(x_0)$ und $f(x_4)$. Sowohl das Intervall (x_0, x_1) als auch das Intervall (x_3, x_4) wäre hiernach ein solches, in welchem $f(x)$ am Anfang und Ende entgegengesetztes Vorzeichen hat, und es könnten also nach dem, was oben bewiesen worden, Werthe x', x'' bestimmt werden, für welche:

$$x_0 < x' < x_1, \quad x_3 < x'' < x_4, \quad |f(x')| < \frac{1}{r}, \quad |f(x'')| < \frac{1}{r}$$

wäre, wenn r beliebig angenommen wird. Nun müsste aber gemäss der Ungleichheit (𝔈.):

$$|f(x')| + \left|\frac{f(x'') - f(x')}{x'' - x'}\right| > \frac{1}{s(s-1)}$$

sein, also, da:

$$|f(x')|<\frac{1}{r},\quad |f(x'')-f(x')|<|f(x'')|+|f(x')|<\frac{2}{r}$$

ist, auch:

$$\frac{1}{r}+\frac{2}{r(x''-x')}>\frac{1}{s(s-1)},$$

und endlich, da:

$$x''-x'>x_2-x_1=\frac{2|f(x_2)|}{(s-1)D}$$

ist:

$$\frac{1}{r}+\frac{(s-1)D}{r|f(x_2)|}>\frac{1}{s(s-1)},$$

oder:

$$r<s(s-1)\left(1+\frac{(s-1)D}{|f(x_2)|}\right).$$

Da aber die Zahl r beliebig gross gewählt werden kann, so kann diese Ungleichheit nicht bestehen, und es ist also in der That zu erschliessen, dass in einem Intervalle, welches nicht grösser als $\frac{1}{s}$ ist, die Function $f(x)$ durchweg einerlei Vorzeichen hat, sobald man nur weiss, dass dies an den beiden Endpunkten der Fall ist.

Nunmehr folgt unmittelbar, dass $f(x)$ in einem Intervalle von der Grösse $\frac{1}{s}$ nicht *mehr* als ein Mal das Zeichen wechseln kann. Denn wäre für drei in dem Intervalle liegende Werthe x_0, x_1, x_2, wofür $x_0<x_1<x_2$ ist:

$$\text{sgn.}\, f(x_0)=-\text{sgn.}\, f(x_1)=\text{sgn.}\, f(x_2),$$

so würde ja das Intervall (x_0, x_2) ein solches sein, dessen Grösse kleiner als $\frac{1}{s}$ wäre, und an dessen Anfangs- und Endpunkt $f(x)$ dasselbe Vorzeichen

hätte. In einem solchen Intervalle kann aber, wie so eben bewiesen worden, $f(x)$ sein Zeichen nicht wechseln; es kann also nicht:

$$\text{sgn.}\, f(x_0)=-\text{sgn.}\, f(x_1)$$

sein.

Das im Vorstehenden entwickelte Resultat kann folgendermaassen formulirt werden:

Erstens sei $a_0+a_1x+a_2x^2+\cdots+a_nx^n$ eine ganzzahlige Function von x, die mit $f(x)$ bezeichnet werden möge; D sei der absolute Werth der Discriminante der Function $f(x)$ und $f'(x)$ ihre Ableitung.

Zweitens seien $\varphi(x)$, $\varphi_1(x)$ ganzzahlige Functionen von x, beziehungsweise von den Graden $n-2$ und $n-1$, für welche die Gleichung:

$$\varphi(x)f(x)+\varphi_1(x)f'(x)=D$$

besteht, und es sei:

$$\varphi(x)=\sum_{k=0}^{k=n-2}\alpha_k x^k,\quad \varphi_1(x)=\sum_{k=0}^{k=n-1}\alpha_k' x^k.$$

Drittens seien mittels der Gleichungen:

$$f(x+y)-f(x)=yf_1(x,y),\quad (f_1(x,y)-f'(x))\varphi(x)=y\psi(x,y)$$

die Functionen $f_1(x, y)$, $\psi(x, y)$ definirt, so dass also in den Entwickelungen:

$$f_1(x,y)=\sum_{h,k}b_{h,k}x^hy^k \qquad (h,\ k=0,1,\ldots n-1),$$

$$\psi(x,y)=\sum_{h,k}c_{h,k}x^hy^k \qquad (h,\ k=0,1,\ldots 2n-4),$$

die Coefficienten b und c ganze Zahlen bedeuten.

Viertens sei $|a_g|$ der grösste der Werthe $|a_0|, |a_1|, \ldots |a_{n-1}|$, und es sei s die kleinste positive ganze Zahl, welche den Ungleichheitsbedingungen:

$$(s-1)D \geqq \sum_h |\alpha_h| \cdot \left(\frac{|a_g|+|a_n|}{|a_n|}\right)^h \qquad (h=0, 1, \ldots n-2),$$

$$(s-1)D \geqq \sum_h |\alpha'_h| \cdot \left(\frac{|a_g|+|a_n|}{|a_n|}\right)^h \qquad (h=0, 1, \ldots n-1),$$

$$(s-1)D \geqq \sum_{h,k} |b_{h,k}| \cdot \left(\frac{|a_g|+|a_n|}{|a_n|}\right)^h \qquad (h, k=0, 1, \ldots n-1),$$

$$(s-1)D \geqq \sum_{h,k} |c_{h,k}| \cdot \left(\frac{|a_g|+|a_n|}{|a_n|}\right)^h \qquad (h, k=0, 1, \ldots 2n-4),$$

genügt.

Alsdann kann nicht $\operatorname{sgn.} f(x') = -\operatorname{sgn.} f(x'') = \operatorname{sgn.} f(x''')$ sein, wenn:

$$x' < x'' < x''' \quad \text{und} \quad x''' - x' \leqq \frac{1}{s}$$

ist; die Function $f(x)$ behält demnach ihr Vorzeichen in jedem Intervalle von der Grösse $\frac{1}{s}$, in welchem die Vorzeichen am Anfangs- und Endpunkt gleich sind, und sie wechselt ihr Vorzeichen nur ein einziges Mal in jedem Intervalle von der Grösse $\frac{1}{s}$, in welchem die Vorzeichen am Anfangs- und Endpunkt verschieden sind. In einem Intervalle der letzteren Art kann ferner, wenn r eine beliebige positive ganze Zahl bedeutet, ein Theilintervall von der Grösse $\frac{1}{rsD}$ so bestimmt werden, dass die Function $f(x)$ am Anfangs- und Endpunkt verschiedenes Vorzeichen hat und durchweg in dem Theilintervalle ihrem absoluten Werthe nach kleiner als $\frac{1}{r}$ bleibt. Endlich behält die Function $f(x)$ das Vorzeichen von $a_n x^n$, sobald x seinem absoluten Werthe nach grösser als $\frac{|a_g|+|a_n|}{|a_n|}$ wird.

Hiernach kann, wenn die ganze Zahl t durch die Ungleichheitsbedingung:

$$s(|a_g|+|a_n|) \leqq t|a_n| < |a_n| + s(|a_g|+|a_n|)$$

bestimmt wird, die Function $f(x)$ nur in einem Intervalle: $\left(\frac{k-1}{s}, \frac{k}{s}\right)$ ihr Zeichen wechseln, in welchem k einen der Werthe: $-t+1, -t+2, \ldots, t-1, t$ hat. Man braucht also nur die Vorzeichen der $2t$ Werthe:

$$f\left(\frac{k}{s}\right) \qquad (k=-t+1, -t+2, \ldots t-1, t)$$

zu bestimmen, um diejenigen der $2t-1$ Intervalle von der Grösse $\frac{1}{s}$ zu ermitteln, in welchen die Function $f(x)$ ihr Zeichen — und zwar nur ein Mal — wechselt. Die Anzahl dieser Intervalle ist zugleich diejenige, welche man als Anzahl der reellen Wurzeln der Gleichung $f(x)=0$ bezeichnet, und es wird also durch das angegebene Verfahren dasjenige vollkommen ersetzt, welches der *Sturm*'sche Satz liefert. Aber auch die sogenannte Berechnung der reellen Wurzeln selbst wird durch das angegebene Verfahren ersetzt; denn wenn sich für eine bestimmte Zahl k zeigt, dass:

$$\operatorname{sgn.} f\left(\frac{k-1}{s}\right) f\left(\frac{k}{s}\right) = -1$$

ist, so braucht man nur die Anfangs- und Endwerthe von $f(x)$ in den Theilintervallen von der Grösse $\frac{1}{rsD}$, d. h. also die $rD+1$ Werthe:

$$f\left(\frac{k}{s} - \frac{h}{rsD}\right) \qquad (h=0, 1, \ldots rD)$$

zu berechnen und diejenige Zahl h zu bestimmen, wofür:

$$\operatorname{sgn.} f\left(\frac{k}{s} - \frac{h}{rsD}\right) f\left(\frac{k}{s} - \frac{h-1}{rsD}\right) = -1$$

ist, um daraus zu erschliessen, dass die Function $f(x)$ in dem Intervalle:

$$\frac{k}{s} - \frac{h}{rsD} \leqq x < \frac{k}{s} - \frac{h-1}{rsD}$$

ihr Zeichen wechselt und absolut durchweg kleiner als $\frac{1}{r}$ bleibt.

Die sogenannte Existenz der reellen irrationalen Wurzeln algebraischer Gleichungen ist einzig und allein in der Existenz von Intervallen der angegebenen Beschaffenheit begründet; die Zulässigkeit der Rechnung mit den einzelnen Wurzeln einer algebraischen Gleichung beruht ganz und gar auf der Möglichkeit sie zu isoliren, also auf der Möglichkeit eine Zahl, wie die oben mit s bezeichnete, zu bestimmen. Ist eine solche Zahl s bestimmt, welche die Eigenschaft hat, dass die Intervalle von der Grösse $\frac{1}{s}$ hinreichend klein sind, um die verschiedenen Wurzeln derselben Gleichung zu isoliren, so wird das „Grösser" und „Kleiner" der Wurzeln einfach durch die Aufeinanderfolge der bezüglichen Isolirungs-Intervalle definirt. Das „Grösser" und „Kleiner" irgend welcher irrationalen algebraischen Zahlen bestimmt sich hiernach auch, wenn man — wie es offenbar zulässig ist — die beiden ihrer Grösse nach zu vergleichenden algebraischen Zahlen sich als zwei Wurzeln einer und derselben Gleichung denkt. Das eigentliche Wesen der Sache tritt aber erst dann in der obigen Deduction vollkommen scharf hervor, wenn man darin auch die Benutzung von Brüchen vermeidet und ausschliesslich von ganzen Zahlen Gebrauch macht.

Wird zu diesem Zwecke an Stelle von $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ die *homogene* ganze Function:

$$a_0 y^n + a_1 y^{n-1} z + a_2 y^{n-2} z^2 + \cdots + a_n z^n$$

eingeführt und mit $F(y, z)$ bezeichnet, so ist:

$$f\left(\frac{x}{y}\right) = \frac{1}{y^n} F(y, z).$$

Es wird also:

$$\text{sgn.}\, F(rsD,\ krD - h) \cdot F(rsD,\ krD - h + 1) = -1,$$

und wenn q eine unbestimmte ganze positive Zahl bedeutet, so wird für alle ganzzahligen Werthe von z die zwischen:

$$(krD - h)q \quad \text{und} \quad (krD - h + 1)q$$

liegen:

$$|F(qrsD, z)| < r^{n-1}(qsD)^n,$$

während das *Vorzeichen* von $F(qrsD, z)$ für $z = (krD - h)q$ entgegengesetzt demjenigen für $z = (krD - h + 1)q$ ist.

Die Zahl s bestimmt sich in der oben angegebenen Weise durch die Coefficienten der Function $F(x, y)$. Alsdann bestimmen sich die verschiedenen ganzzahligen Werthe von k, welche die verschiedenen reellen Wurzeln der Gleichung $f(x) = 0$ charakterisiren, durch die Bedingung:

$$\text{sgn.}\, F(s, k-1) \cdot F(s, k) = -1.$$

Wird nun noch eine Zahl r beliebig angenommen, so wird die zu einem bestimmten Werthe von k gehörige positive und rD nicht übersteigende Zahl h durch die Bedingung:

$$\text{sgn.}\, F(rsD,\ krD - h) \cdot F(rsD,\ krD - h + 1) = -1$$

definirt, und es ist alsdann:

$$|F(rsD,\ krD - h)| < r^{n-1}(sD)^n,$$
$$|F(rsD,\ krD - h + 1)| < r^{n-1}(sD)^n.$$

Jede der reellen Wurzeln der Gleichung $f(x) = 0$ wird also durch je eine bestimmte Zahl k vollkommen charakterisirt; alsdann aber gehört zu jeder beliebig angenommenen Zahl r noch je eine bestimmte Zahl h, und man kann also die Zahlen h als „Functionen der unbestimmten ganzen Zahlen r" auffassen, welche durch die ganzzahlige Function $F(y, z)$ definirt werden.

In den Resultaten der „allgemeinen Arithmetik" oder der „arithmetischen Theorie der ganzen ganzzahligen Functionen von Unbestimmten" kann man nur eine Zusammenfassung aller derjenigen Resultate sehen, welche sich ergeben, wenn man den Unbestimmten ganzzahlige Werthe beilegt. Insofern gehören also auch die Resultate der *allgemeinen* Arithmetik eigent-

lich der speciellen gewöhnlichen Zahlentheorie an, und alle Ergebnisse der tiefsinnigsten mathematischen Forschung müssen schliesslich in jenen einfachen Formen der Eigenschaften ganzer Zahlen ausdrückbar sein. Aber um diese Formen einfach erscheinen zu lassen, bedurfte es vor Allem einer geeigneten übersichtlichen Ausdrucks- und Darstellungsweise für die Zahlen selbst, und hieran hat der Menschengeist gewiss seit grauer Vorzeit anhaltend und mühsam, bald mehr bald weniger erfolgreich, und je nach den verschiedenen Völkerschaften in ganz verschiedener Weise gearbeitet*). Die Frucht dieser Arbeit, unsere Wort- und Ziffer-Bezeichnung der Zahlen, war ebenso wohl die Vorbedingung für die Auffindung des Wissensschatzes, über den die heutige Arithmetik verfügt, wie für die Aufstellung jener „Gesetze, in welche wir unsere Kenntniss von der Bewegung der Himmelskörper fassen"; sie war aber auch die Vorbedingung für die ganze jetzige Gestaltung des praktischen Lebens, für die ungeheure Ausbreitung und Ausbildung von Handel und Verkehr, welche die moderne Welt so wesentlich von der alten unterscheidet.

*) Vgl. die Abhandlung *Alexander v. Humboldt*'s: Ueber die bei verschiedenen Völkern üblichen Systeme von Zahlzeichen und über den Ursprung des Stellenwerthes in den indischen Zahlen. (Vorgelesen in einer Klassen-Sitzung der Königl. Akademie der Wissenschaften zu Berlin, den 2. März 1829; abgedruckt im 4. Bande dieses Journals S. 205 ff.)

In dieser Abhandlung wird eine Bemerkung von *Laplace* (in deutscher Uebertragung) citirt, welche im Originaltext[1]) *so* lautet: »C'est de l'Inde que nous vient l'ingénieuse méthode d'exprimer tous les nombres avec dix caractères, en leur donnant à la fois une valeur absolue et une valeur de position; idée fine et importante, qui nous paraît maintenant si simple, que nous en sentons à peine le mérite. Mais cette simplicité même, et l'extrême facilité qui en résulte pour tous les calculs, placent notre système d'arithmétique au premier rang des inventions utiles; et l'on appréciera la difficulté d'y parvenir, si l'on considère qu'il a échappé au génie d'Archimède et d'Apollonius, deux des plus grands hommes dont l'antiquité s'honore.«

[1]) *Laplace*, Exposition du système du monde, sixième édition p. 376. Oeuvres complètes de *Laplace* t. VI p. 404—405. H.

ZUR THEORIE DER GATTUNGEN RATIONALER FUNCTIONEN VON MEHREREN VARIABELN.

VON

L. KRONECKER.

Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin vom Jahre 1886. S. 251—253.

ZUR THEORIE DER GATTUNGEN RATIONALER FUNCTIONEN VON MEHREREN VARIABELN.

[Gelesen in der Akademie der Wissenschaften am 25. Februar 1886.]

Als ich vor nun fünfundzwanzig Jahren in die Akademie eintrat, hatte ich eben eine algebraische Frage zum Abschluss gebracht, deren Erledigung für die weitere Erforschung der Theorie der algebraischen Gleichungen nothwendig war. Ich habe darüber in der Gesammtsitzung vom 27. Juni 1861 eine ausführliche, im Monatsbericht (S. 609—617) abgedruckte, Mittheilung gemacht und dann in der Gesammtsitzung vom 24. October eine grössere Abhandlung über denselben Gegenstand vorgetragen, welche ich zwar nicht habe abdrucken lassen, deren hauptsächlichen Inhalt ich aber bald darauf in meinen Universitätsvorlesungen bekannt gegeben habe. An einer Veröffentlichung durch den Druck hat mich namentlich die Schwierigkeit gehindert, meine bezüglichen Entwickelungen, welche von einer rein arithmetischen Behandlung der algebraischen Grössen ausgingen, in der damals gebräuchlichen, aus analytisch-geometrischer Anschauungsweise hervorgegangenen algebraischen Terminologie auseinanderzusetzen*). Da ich aber nunmehr in

*) Vergl. die Stelle in der Vorrede des »Traité des substitutions et des équations algébriques« von Hrn. *C. Jordan* (Paris, 1870) S. VIII, worin es heisst: »Nous devons à *M. Kronecker* la notion du groupe des équations de la division de ces dernières fonctions. Nous aurions désiré tirer un plus grand parti que nous ne l'avons fait des travaux de cet illustre auteur sur les équations. Diverses causes nous en ont empêché: la nature tout arithmétique de ses méthodes, si différentes de la nôtre; la difficulté de reconstituer intégralement une suite de démonstrations le plus souvent à peine indiquées; enfin l'espérance de voir grouper un jour en un corps de doctrine suivi et complet ces beaux théorèmes qui font maintenant l'envie et le désespoir des géomètres.«

meiner Festschrift zu Hrn. *Kummer*'s Doctorjubiläum[1]), in welcher ein grosser Theil meiner erwähnten, am 24. October 1861 vorgetragenen Abhandlung mit aufgenommen ist, die für eine arithmetische Theorie der algebraischen Grössen geeignete Terminologie eingeführt und die Theorie der Gattungen rationaler Functionen von mehreren Variabeln sowie der Divisorensysteme in ihren Elementen entwickelt habe, bin ich im Stande, den Inhalt meiner Mittheilung vom 27. Juni 1861 in übersichtlicher Weise darzulegen und vollständig zu begründen. Eine besondere Veranlassung dazu ist mir jetzt dadurch geworden, dass ich bei den Vorbereitungen für Universitätsvorlesungen, welche ich in diesem Winter über denselben Gegenstand halte, nicht nur mancherlei Verbesserungen meiner früheren Methoden, sondern auch einige neue Resultate erlangt habe, von denen ich eines gleich hier hervorheben will.

In meiner Mittheilung vom 27. Juni 1861*) habe ich als das Wesentliche in der Theorie der Gleichungen fünften Grades bezeichnet, „dass es unter den zehnwerthigen rationalen Functionen von fünf Grössen: x_0, x_1, x_2, x_3, x_4, welche bei allen cyklischen Permutationen von je drei dieser Grössen nur fünf Werthe annehmen, solche giebt, für welche die symmetrischen Functionen dieser fünf Werthe nur von *zwei* Functionen der Grössen x abhängen", und ich habe bemerkt, dass dies schon aus den einfachsten Betrachtungen über die dort behandelten Functionen $f(x_k, x_{k+3}, x_{k+4}, x_{k+1}, x_{k+2})$ hervorgehe. Eben dasselbe Resultat lässt sich aber auch direct und unabhängig von der Theorie der Functionen f in der folgenden eleganten Weise herleiten.

Bezeichnet man die rationale Function:

$$\frac{(x_1 - x_2)\,(x_3 - x_4)}{(x_1 - x_3)\,(x_2 - x_4)}$$

mit $\Theta(x_1, x_2, x_3, x_4)$, so ist offenbar für jeden beliebigen Werth von r:

$$\Theta(x_1, x_2, x_3, x_4) = \Theta(x_1 + r, x_2 + r, x_3 + r, x_4 + r)$$

*) Monatsbericht S. 613.

[1]) Band II S. 237—387 dieser Ausgabe. H.

und auch:

$$\Theta(x_1, x_2, x_3, x_4) = \Theta\left(\frac{1}{x_1}, \frac{1}{x_2}, \frac{1}{x_3}, \frac{1}{x_4}\right).$$

Folglich besteht die Relation:

$$\Theta(x_1, x_2, x_3, x_4) = \Theta(y_1, y_2, y_3, y_4),$$

wenn:

$$y_k = \frac{a x_k + b}{c x_k + d} \qquad (k = 1, 2, 3, 4)$$

ist und a, b, c, d beliebige Grössen bedeuten. Man kann also z. B. a, b, c, d so bestimmen, dass $y_2 = -1$, $y_3 = 0$, $y_4 = +1$ wird, indem man:

$$y_k = \frac{(x_k - x_3)\,(x_2 - x_4)}{(x_k - x_2)\,(x_3 - x_4) + (x_k - x_4)\,(x_3 - x_2)} \qquad (k = 1, 2, 3, 4)$$

setzt.

Nimmt man nun zu den Variabeln x_1, x_2, x_3, x_4 noch eine Variable x_0 hinzu, so sind offenbar die sämmtlichen Functionen:

$$\Theta(x_\alpha, x_\beta, x_\gamma, x_\delta),$$

welche entstehen, indem man für $\alpha, \beta, \gamma, \delta$ je vier unter einander verschiedene von den Zahlen 0, 1, 2, 3, 4 setzt, nur Functionen der *zwei* Grössen y_0 und y_1 oder:

$$\frac{(x_0 - x_3)\,(x_2 - x_4)}{(x_0 - x_2)\,(x_3 - x_4) + (x_0 - x_4)\,(x_3 - x_2)}, \qquad \frac{(x_1 - x_3)\,(x_2 - x_4)}{(x_1 - x_2)\,(x_3 - x_4) + (x_1 - x_4)\,(x_3 - x_2)};$$

welche selbst rationale Functionen von x_0, x_1, x_2, x_3, x_4 sind. Die Coefficienten der Gleichung, welcher alle diese conjugirten Functionen Θ genügen, hängen also nur von *zwei* rationalen Functionen der fünf Grössen x ab.

Aus den Functionen Θ kann leicht eine solche gebildet werden, die bei allen cyklischen Permutationen von drei Grössen x fünf verschiedene

Werthe annimmt, deren symmetrische Functionen nur von zwei Functionen der Grössen x abhängen. Solche fünf conjugirte Functionen von x_0, x_1, x_2, x_3, x_4 erhält man z. B., wenn man zu dem Product-Ausdrucke:

$$\left(\frac{x_1-x_4}{x_1-x_3}+\frac{x_2-x_4}{x_2-x_3}\right)\cdot\left(\frac{x_1-x_2}{x_1-x_4}+\frac{x_3-x_2}{x_3-x_4}\right)\cdot\left(\frac{x_1-x_3}{x_1-x_2}+\frac{x_4-x_3}{x_4-x_2}\right)$$

die vier übrigen conjugirten bildet. Diese fünf conjugirten Functionen sind offenbar solche, wie ich sie in dem obigen Citat aus meiner Mittheilung vom 27. Juni 1861 als existent hervorgehoben habe; sie genügen einer Gleichung fünften Grades, deren Coefficienten zweiwerthige rationale Functionen der fünf Grössen x sind und nur von *zwei* solchen Functionen abhängen, und sie entstehen — wie ich noch bemerken will — ganz einfach, indem die zweite Invariante je einer der Gleichungen vierten Grades, welche aus der Gleichung fünften Grades:

$$(x-x_0)(x-x_1)(x-x_2)(x-x_3)(x-x_4)=0$$

bei Adjunction je einer der Grössen x_0, x_1, x_2, x_3, x_4 hervorgehen, durch die Quadratwurzel aus der Discriminante dividirt wird.

ÜBER DIE ARITHMETISCHEN SÄTZE, WELCHE LEJEUNE DIRICHLET IN SEINER BRESLAUER HABILITATIONSSCHRIFT ENTWICKELT HAT.

VON

L. KRONECKER.

Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin vom Jahre 1888. S. 417—423.

ÜBER
DIE ARITHMETISCHEN SÄTZE, WELCHE LEJEUNE DIRICHLET IN SEINER BRESLAUER HABILITATIONSSCHRIFT ENTWICKELT HAT.

[Gelesen in der Akademie der Wissenschaften am 5. April 1888.]

Auf die erste, am 11. Juli 1825 der Pariser Akademie überreichte, arithmetische Abhandlung *Lejeune Dirichlet*'s folgte 1827 eine zweite, mit welcher er sich in Breslau habilitirte[1]). Sie ist in Octavformat (ohne Angabe der Jahreszahl) gedruckt und wohl nur in wenigen Exemplaren hergestellt worden. Auf dem Titelblatte steht:

»*De formis linearibus, in quibus continentur divisores primi quarumdam formularum graduum superiorum commentatio, quam ad veniam docendi ab amplissimo philosophorum ordine in regia universitate litterarum Vratislaviensi impetrandam conscripsit Gustavus Lejeune Dirichlet, philosophiae doctor. Vratislaviae, typis Kupferianis.*«

Den Ausgangspunkt bildet die Bemerkung, dass die Primtheiler jeder Form zweiten Grades durch gewisse Linearformen charakterisirt seien, dass dies aber, wenn der Grad grösser als 2 ist, nur für besondere Formen, wie z. B. für die von *Euler* untersuchten Formen $x^n \pm 1$ der Fall sei. Bei der Beschäftigung mit diesen *Euler*'schen Untersuchungen, sagt *Dirichlet* am Schlusse der Einleitung, sei er auf eine neue Art von Formen höheren Grades gekommen, welche ähnliche Eigenschaften wie die von *Euler* behandelten besitzen.

[1]) *G. Lejeune-Dirichlet* gesammelte Werke Bd. I S. 47—62.

Es sind dies die Formen U und V, welche entstehen, wenn man den Ausdruck $(x+V\overline{b})^n$ auf die Form $U+VV\overline{b}$ bringt. Dabei bedeutet x eine „Unbestimmte", n eine beliebige positive ganze Zahl und b eine positive oder negative ganze Zahl, welche nur kein vollständiges Quadrat sein darf.

Dirichlet untersucht und bestimmt die Primtheiler von V unter der Voraussetzung, dass n eine Primzahl ist, und die von U für den Fall, dass n eine Potenz von 2 ist. Er bemerkt dabei, dass seine Untersuchungs-Methode auch bei jedem andern ganzzahligen Werthe von n anwendbar sei, dass er sich aber, um der Abhandlung keine zu grosse Ausdehnung zu geben, auf jene beiden Fälle beschränken wolle.

Als ich nun beim Abdruck jener Habilitationsschrift in *Lejeune Dirichlet*'s Werken zu eingehender Beschäftigung mit derselben veranlasst wurde, machte ich den Versuch, das von *Dirichlet* behandelte Problem mit Hülfe von Modulsystemen auf rein arithmetischem und ganz im absoluten Rationalitätsbereich der gewöhnlichen Zahlen bleibendem Wege zu lösen. Dies gelang in überraschend einfacher Weise, und dabei ganz vollständig, d. h. für jeden beliebigen Werth der Zahlen b und n. Wenn nun auch jenes *Dirichlet*'sche arithmetische Problem selbst jetzt als ein elementares zu betrachten ist, so wird doch eine kurze Auseinandersetzung der neuen und ganz allgemeinen Lösung hauptsächlich durch das Interesse, welches sich an jeden von *Dirichlet* behandelten Gegenstand knüpft, dann aber auch als ein neuer Beleg für die Anwendbarkeit der Modulsysteme wohl gerechtfertigt erscheinen.

I. Bedeutet n eine positive ganze Zahl und z eine unbestimmte Variable, so hat z^n-1 so viel verschiedene ganze ganzzahlige Factoren als n verschiedene Divisoren hat. Einer dieser Factoren, welcher als der „primitive" bezeichnet werden soll, ist dadurch vollständig charakterisirt, dass er nicht zugleich als Factor in irgend einem Ausdrucke z^m-1 enthalten ist, in welchem der Exponent m kleiner als n ist.

Es sei nun, wie in meiner Mittheilung vom 29. Juli 1886*),

*) Zur Theorie der elliptischen Functionen, Art. XI, § 2. Sitzungsbericht von 1886, S. 707.

$$\varepsilon_1=1,\quad \varepsilon_m=(-1)^\nu,$$

wenn die Zahl m lauter verschiedene Primzahlen enthält und ν deren Anzahl bedeutet, aber

$$\varepsilon_m=0,$$

wenn m irgend eine Primzahl mehrfach enthält. Ferner sei $F_m(z)$ der primitive Factor von z^m-1. Alsdann ist:

(A) $$F_n(z)=\prod_d (z^{\frac{n}{d}}-1)^{\varepsilon_d},\quad z^n-1=\prod_d F_d(z),$$

wo die Multiplication über alle Divisoren d von n zu erstrecken ist. Setzt man endlich:

$$(x+y)^{\frac{n}{d}}-(x-y)^{\frac{n}{d}}=yf_d(x,y^2),$$

wo x und y unbestimmte Variable bedeuten und $f_d(x,y^2)$ eine ganze ganzzahlige Function von x und y^2 ist, so wird:

$$(x-y)^{\varphi(n)}F_n\left(\frac{x+y}{x-y}\right)=\prod_d f_d(x,y^2)^{\varepsilon_d}$$ (d alle Divisoren von n)

da die über alle Divisoren d von n erstreckte Summe $\sum\varepsilon_d$ gleich Null ist, und es zeigt sich also, dass der Ausdruck auf der linken Seite der Gleichung, der offenbar eine ganze ganzzahlige Function von x und y ist, nur die graden Potenzen von y enthält. Bezeichnet man denselben zur Abkürzung durch:

$$G_n(x,y^2),$$

so ist es die ganze ganzzahlige Function:

$$G_n(x,s),$$

deren Primtheiler q für beliebig angenommene positive oder negative ganzzahlige Werthe von s zu bestimmen sind.

Die Form $G_n(x, s)$ ist offenbar, wie die Function $F_n(x)$, vom Grade $\varphi(n)$, wo $\varphi(n)$ in üblicher Weise die Anzahl derjenigen unter einander *modulo* n incongruenten Zahlen bedeutet, die zu n relativ prim sind.

II. Bilden $r_1, r_2, \ldots$ ein vollständiges System derjenigen unter einander *modulo* n incongruenten Zahlen, die zu n relativ prim sind, so findet die Congruenz:

$$\text{(B)} \qquad \prod_r (x - z^r) \equiv F_n(x) \pmod{F_n(z)} \qquad (r = r_1, r_2, \ldots)$$

statt. Um dies darzuthun, soll zuvörderst gezeigt werden, dass:

$$F_n(z^r) \equiv 0 \pmod{F_n(z)}$$

ist. In der That ist gemäss den Gleichungen (A):

$$z^{rn} - 1 = \prod_r F_d(z^r) \equiv 0 \pmod{F_n(z)} \qquad (d \text{ alle Divisoren von } n),$$

und keiner der Factoren $F_d(z^r)$, bei welchem $d < n$ ist, hat einen gemeinsamen Theiler mit $F_n(z)$. Derselbe Theiler müsste nämlich in jeder der beiden Functionen: $z^{rd} - 1$ und $z^n - 1$, also auch in $z^{ard+bn} - 1$ enthalten sein. Da man nun die Zahlen a, b so bestimmen kann, dass $ard + bn = d$ wird, so müssten $F_n(z)$ und $z^d - 1$, also auch $F_n(z)$ und $F_t(z)$ einen gemeinsamen Theiler haben, wo t einen Divisor von d bedeutet. Zwei Functionen $F_d(z)$, welche verschiedenen Divisoren d entsprechen, können aber keinen gemeinsamen Theiler haben, da ihr Product in $z^n - 1$ als Theiler enthalten ist, und da $z^n - 1$ mit der Ableitung nz^{n-1} keinen gemeinsamen Theiler hat.

Aus der Congruenz: $F_n(z^{r_1}) \equiv 0 \pmod{F_n(z)}$ folgt:

$$F_n(x) \equiv (x - z^{r_1})\, \Phi(x, z) \pmod{F_n(z)},$$

wo $\Phi(x, z)$ eine ganze ganzzahlige Function von x und z ist. Da ferner:

$$F_n(z^{r_2}) \equiv 0, \quad \text{also} \quad (z^{r_2} - z^{r_1})\, \Phi(z^{r_2}, z) \equiv 0 \pmod{F_n(z)}$$

ist, so muss:

$$\Phi(z^{r_2}, z) \equiv 0 \pmod{F_n(z)}$$

und folglich $\Phi(x, z)$ *modulo* $F_n(z)$ durch $x - z^{r_2}$ theilbar sein. Denn der Factor $z^{r_2} - z^{r_1}$ hat mit $F_n(z)$ keinen gemeinsamen Theiler, da ein solcher Theiler sonst auch in $z^d - 1$ enthalten sein müsste, wenn d den grössten in $r_1 - r_2$ enthaltenen Divisor von n bedeutet; und dass $F_n(z)$ und $z^d - 1$ keinen gemeinsamen Theiler haben, ist soeben dargethan worden.

Es erweist sich also $F_n(x)$ als *modulo* $F_n(z)$ durch das Product $(x - z^{r_1})(x - z^{r_2})$ theilbar, und indem man so fortfährt, erschliesst man offenbar die Richtigkeit der oben aufgestellten Congruenz (B).

III. Auf Grund der Congruenz (B) ergiebt sich für die zu untersuchende Function $G_n(x, s)$ ganz unmittelbar die Congruenz:

$$\text{(C)} \qquad G_n(x, s) \equiv \prod_r ((x + y) - (x - y)\, z^r) \pmod{y^2 - s,\ F_n(z)} \qquad (r = r_1, r_2, \ldots),$$

und die oben mit q bezeichneten Primtheiler der Form $G_n(x, s)$ werden also durch die Forderung bestimmt, dass ganzzahlige Werthe von x existiren sollen, für welche die Congruenz:

$$\prod_r (x + y - (x - y)\, z^r) \equiv 0 \pmod{q,\ y^2 - s,\ F_n(z)} \qquad (r = r_1, r_2, \ldots)$$

erfüllt wird. Hierfür ist offenbar nothwendig und hinreichend, dass die Congruenz:

$$\text{(D)} \qquad \prod_k \prod_r (k + y - (k - y)\, z^r) \equiv 0 \pmod{q,\ y^2 - s,\ F_n(z)} \qquad \left(\begin{smallmatrix} r = r_1, r_2, \ldots \\ k = 0, 1, \ldots q-1 \end{smallmatrix}\right)$$

bestehe. Da nun:

$$\prod_k (u - kv) \equiv u^q - uv^{q-1} \pmod{q} \qquad (k = 0, 1, \ldots q-1)$$

ist, so geht die Congruenz (D) in folgende über:

$$\prod_r (y^q (z^r+1)^q - y (z^r+1)(z^r-1)^{q-1}) \equiv 0 \pmod{q,\ y^2-s,\ F_n(z)} \qquad (r=r_1, r_2, \ldots),$$

und daraus resultirt, wenn man jeden Factor des Products auf der linken Seite mit z^r-1 multiplicirt und die Congruenzen:

$$(z^r+1)^q \equiv z^{rq}+1 \pmod{q}$$

$$y^{q-1} \equiv s^{\frac{1}{2}(q-1)} \equiv \left(\frac{s}{q}\right) \pmod{q,\ y^2-s}$$

benutzt, die Congruenz:

$$\prod_r ((z^{r(q+1)}-1)(1-\sigma) + z^r (z^{r(q-1)}-1)(1+\sigma)) \equiv 0 \pmod{q,\ F_n(z)}$$
$$(r=r_1, r_2, \ldots),$$

in welcher zur Abkürzung der Werth des *Legendre*'schen Zeichens $\left(\frac{s}{q}\right)$ mit σ bezeichnet ist. Je nachdem $\sigma=+1$ oder $\sigma=-1$ ist, muss daher die Congruenz:

$$\prod_r (z^{r(q-1)}-1) \equiv 0 \quad \text{oder} \quad \prod_r (z^{r(q+1)}-1) \equiv 0 \pmod{q,\ F_n(z)} \qquad (r=r_1, r_2, \ldots)$$

stattfinden, d. h. es muss:

$$\text{(E)} \qquad \prod_r (z^{r(q-\sigma)}-1) \equiv 0 \pmod{q,\ F_n(z)}$$

sein.

Das Divisorensystem:

$$(q,\ F_n(z),\ z^{r(q-\sigma)}-1) \quad \text{oder} \quad (q,\ F_n(z),\ z^n-1,\ z^{r(q-\sigma)}-1),$$

ist offenbar aequivalent $(q,\ F_n(z),\ z^d-1)$, wenn d den grössten in $q-\sigma$ enthaltenen Divisor von n bedeutet, und es soll nun gezeigt werden, dass dieses Divisorensystem aequivalent *Eins* ist, wenn $d<n$ ist. Alsdann besteht nämlich die Congruenz:

$$\frac{z^n-1}{z^d-1} \equiv 0 \pmod{F_n(z)},$$

da z^n-1 durch $F_n(z)$ theilbar ist und $F_n(z)$, wie oben bewiesen worden, mit z^d-1 keinen Factor gemein hat. In jenem Divisorensysteme kann also das Element $\frac{z^n-1}{z^d-1}$ hinzugefügt werden, und da:

$$\frac{z^n-1}{z^d-1} \equiv \frac{n}{d} \pmod{z^d-1}$$

ist, auch das Element $\frac{n}{d}$. Das Divisorensystem wird hiernach:

$$\left(q,\ \frac{n}{d},\ F_n(z),\ z^{r(q-\sigma)}-1\right),$$

und dies ist in der That aequivalent *Eins*, wenn — wie jetzt vorausgesetzt werden soll — die Primzahl q nicht in n enthalten ist.

Da nun vermöge der Congruenz (E) das über alle Werthe von r erstreckte Product der Divisorensysteme:

$$(q,\ F_n(z),\ z^{r(q-\sigma)}-1)$$

das Modulsystem $(q,\ F_n(z))$ enthalten soll, so können diese Divisorensysteme nicht sämmtlich aequivalent *Eins* sein, und es muss also der mit d bezeichnete, grösste in $q-\sigma$ enthaltene Divisor von n gleich n selbst sein; d. h. es muss die Congruenz

$$q \equiv \sigma \equiv \left(\frac{s}{q}\right) \pmod{n}$$

bestehen. Da aber auch andererseits, wenn diese Congruenz besteht, jeder einzelne Factor des Products:

$$\prod_{r}(z^{r(q-\varrho)}-1) \qquad (r=r_1, r_2, \ldots)$$

durch $F_n(z)$ theilbar ist, so ergiebt sich als Endresultat,

dass die Primtheiler q der Form $G_n(x, s)$, welche nicht in n enthalten sind, sämmtlich durch die Congruenz:

$$q \equiv \left(\frac{s}{q}\right) \pmod{n}$$

charakterisirt werden.

Da die Primzahlen q, für welche $\left(\frac{s}{q}\right)$ den einen oder den anderen Werth hat, bestimmte Linearformen in Beziehung auf $4s$ haben, so werden die nicht in n enthaltenen Primtheiler von $G_n(x, s)$ zugleich in Beziehung auf n und $4s$, also in Beziehung auf die kleinste durch n und $4s$ theilbare Zahl t, durch bestimmte Linearformen charakterisirt, d. h. durch eine Reihe von Linearformen:

$$kt+\varrho', \quad kt+\varrho'', \quad kt+\varrho''', \ldots,$$

in welchen ϱ', ϱ'', ϱ''', ... gewisse Reste von t bedeuten.

IV. Im Anschluss an die *Dirichlet*'sche Abhandlung möge noch der besondere Fall erörtert werden, in welchem n durch s theilbar und s ungrade ist.

Alsdann muss

für $q \equiv +1 \pmod{n}$ zugleich $\left(\frac{s}{q}\right) = +1$ und $\left(\frac{q}{s}\right) = 1$,

für $q \equiv -1 \pmod{n}$ aber $\left(\frac{s}{q}\right) = -1$ und $\left(\frac{q}{s}\right) = \left(\frac{-1}{s}\right)$

sein.

Ist nun erstens $q \equiv 1 \pmod{4}$, so ist $\left(\frac{s}{q}\right) = \left(\frac{q}{s}\right)$, und es muss also für $q \equiv -1 \pmod{n}$ auch $|s| \equiv -1 \pmod{4}$ sein, d. h. der absolute Werth von s muss von der Form $4k-1$ sein.

Ist zweitens $q \equiv -1 \pmod{4}$, so ist:

$$\left(\frac{s}{q}\right) = -\left(\frac{q}{s}\right)(-1)^{\frac{1}{2}(s-1)},$$

es muss also für $q \equiv 1 \pmod{n}$ die Congruenz $s \equiv 1 \pmod{4}$ bestehen, und für $q \equiv -1 \pmod{n}$ muss s negativ sein.

Für jeden Werth von s können also Primtheiler q, die $\equiv 1 \pmod{n}$ und $\equiv 1 \pmod{4}$ sind, auftreten, aber Primtheiler q mit den Bedingungen:

$q \equiv -1 \pmod{n}$, $q \equiv +1 \pmod{4}$ nur für $|s| \equiv -1 \pmod{4}$,

$q \equiv +1 \pmod{n}$, $q \equiv -1 \pmod{4}$ nur für $s \equiv +1 \pmod{4}$,

$q \equiv -1 \pmod{n}$, $q \equiv -1 \pmod{4}$ nur für $s < 0$.

Ist zugleich s negativ und von der Form $4k-1$, so ist $|s| \equiv 1 \pmod{4}$, und es kann daher nur

entweder: $q \equiv +1 \pmod{n}$, $q \equiv +1 \pmod{4}$

oder: $q \equiv -1 \pmod{n}$, $q \equiv -1 \pmod{4}$

sein. Da überdies:

$$q \equiv \left(\frac{s}{q}\right) \pmod{n}$$

ist, so werden also die Primtheiler q der Form $G_n(x, s)$ für den Fall:

$$s < 0, \quad s \equiv -1 \pmod{4}, \quad n \equiv 0 \pmod{s}$$

dadurch charakterisirt, dass sowohl *modulo* n als auch *modulo* 4 und folglich, wenn n ungrade ist, *modulo* $4n$:

$$q \equiv \left(\frac{s}{q}\right)$$

sein muss. Dieses Resultat findet sich in der *Dirichlet*'schen Habilitationsschrift für den Fall, wo n Primzahl und also gleich dem absoluten Werthe von s ist.

ÜBER SYMMETRISCHE SYSTEME.

VON

L. KRONECKER.

Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin vom Jahre 1889. S. 349—362.

ÜBER SYMMETRISCHE SYSTEME.

[Gelesen in der Akademie der Wissenschaften am 25. April 1889.]

Als ich in meinen Untersuchungen über die Charakteristik von Functionensystemen, welche ich in den Monatsberichten der Akademie vom 14. und 21. Februar 1878[1]) auszugsweise mitgetheilt habe, die Veränderungen betrachtete, welche die Charakteristik bei Variation der Functionen erfährt, wurde ich auf die Frage geführt, ob es möglich sei, von jedem System zu jedem anderen, welches dieselbe Charakteristik hat, durch allmähliche Variation der Functionen so überzugehen, dass dabei die Charakteristik immer ihren Werth beibehält. Nimmt man wie a. a. O. die Functionen von v Parametern $x_1, x_2, \ldots x_v$ abhängig an und definirt also jedes einzelne Functionensystem durch einen einzelnen Punkt der v-fachen Mannigfaltigkeit (x), so erfüllen die Functionensysteme, welche dieselbe Charakteristik haben, gewisse v-fach ausgedehnte Gebiete der v-fachen Mannigfaltigkeit (x), und jene Frage kann alsdann dahin formulirt werden, ob jedes dieser Gebiete zusammenhängend ist.

Ich habe die bezeichnete Frage, welche meines Wissens früher noch nicht erörtert worden ist, für die Charakteristik eines Systems zweier Functionen einer Variabeln in meiner erwähnten Mittheilung im Monatsbericht von 1878 und schon vorher in meinen Universitätsvorlesungen behandelt, namentlich in dem Falle, wo die eine der Functionen die Ableitung der anderen ist und die Charakteristik also durch die Anzahl der reellen Linear-

[1]) Ueber *Sturm*'sche Functionen, Bd. II S. 37—70; Ueber die Charakteristik von Functionensystemen, Bd. II S. 71—82 dieser Ausgabe von *L. Kronecker*'s Werken. H.

factoren der letzteren Function bestimmt wird. Aber in den Universitätsvorlesungen, welche ich in dem vorigen Wintersemester über die Theorie der algebraischen Gleichungen gehalten habe, bin ich, bei Behandlung der Charakteristik von Systemen zweier *beliebigen* ganzen Functionen einer Variabeln mittels der *Jacobi-Bézout*'schen Eliminationsmethode darauf geführt worden, die Gebiete zu untersuchen, in welche eine durch die $\frac{1}{2}n(n+1)$ variabeln Elemente eines symmetrischen Systems:

$$(z_{ik}) \qquad (i, k=1, 2, \ldots n;\ z_{ik}=z_{ki})$$

repräsentirte $\frac{1}{2}n(n+1)$-fache Mannigfaltigkeit zerlegt wird, wenn die Determinante $|z_{ik}|$ gleich Null gesetzt und also die hierdurch dargestellte $\left(\frac{1}{2}n(n+1)-1\right)$-fache Mannigfaltigkeit gebildet wird.

Um die Ergebnisse dieser Untersuchung hier einfach auseinanderzusetzen, schicke ich einige vorbereitende Entwickelungen voraus.

I. Aus der Composition von Systemen:

$$(a_{ik})\ (z_{ik})\ (b_{ik}) \qquad (i, k=1, 2, \ldots n)$$

resultirt, wenn das eine der Systeme (a_{ik}), (b_{ik}) das transponirte des anderen, also:

$$b_{ik}=a_{ki} \qquad (i, k=1, 2 \ldots n)$$

ist, ein symmetrisches System:

$$(z'_{ik}) \qquad (i, k=1, 2, \ldots n).$$

Denn aus der wirklichen Darstellung des Resultats der Composition:

$$\sum_{h,\,i} a_{gh} z_{hi} b_{ik} = \sum_{h,\,i} a_{gh} z_{hi} a_{ki} = z'_{gk} \qquad (g, h, i, k=1, 2, \ldots n)$$

ersieht man unmittelbar, dass aus der Gleichung:

$$z_{hi}=z_{ih} \qquad (h, i=1, 2, \ldots n)$$

die Relation:

$$z'_{gk}=z'_{kg} \qquad (g, k=1, 2, \ldots n)$$

folgt.

II. Wählt man für das System (a_{gh}) ein solches:

$$\left(a^{(t)}_{g,h}\right) \qquad (g, h=1, 2, \ldots n),$$

für welches:

$$a^{(t)}_{11}=a^{(t)}_{22}=a^{(t)}_{33}=\cdots=a^{(t)}_{nn}=1,$$

ferner für einen einzigen Index r:

$$a^{(t)}_{1r}=t$$

und jedes der übrigen Elemente a_{gh} gleich Null wird, so ist:

$$\begin{aligned} z'_{11} &= z_{11}+2tz_{1r}+t^2 z_{rr} \\ z'_{1k} &= z'_{k1}=z_{1k}+tz_{rk} \qquad (k=2, 3, \ldots n) \\ z'_{gk} &= z'_{kg}=z_{gk} \qquad (g, k=2, 3, \ldots n). \end{aligned}$$

Das componirte System z'_{gk} enthält also nur in der ersten Horizontalreihe und in der ersten Verticalreihe Elemente, die von den bezüglichen Elementen z_{gk} verschieden sind.

III. Bedeutet (b_{gh}), wie oben, das transponirte des Systems (a_{gh}), so ist:

$$b^{(t)}_{11}=b^{(t)}_{22}=b^{(t)}_{33}=\cdots=b^{(t)}_{nn}=1,\ \ b^{(t)}_{r1}=t,$$

und jedes der übrigen Elemente b_{gh} wird gleich Null. Bezeichnet man nun das System, welches aus der Composition:

$$\left(b_{ik}^{(t)}\right)\left(z_{ik}\right)\left(a_{ik}^{(t)}\right) \qquad (t,\ k=1,\ 2,\ \ldots n)$$

resultirt, mit:

$$\left(z_{ik}''\right) \qquad (g,\ k=1,\ 2,\ \ldots n),$$

so ist:

$$z_{rr}'' = z_{rr} + 2tz_{1r} + t^2 z_{11},$$

$$z_{rk}'' = z_{kr}'' = z_{kr} + tz_{k1} \qquad (k=1,\ 2,\ \ldots r-1,\ r+1,\ \ldots n)$$

$$z_{gk}'' = z_{kg}'' = z_{gk} \qquad (g,\ k=1,\ 2,\ \ldots r-1,\ r+1,\ \ldots n).$$

Das componirte System z_{gk}'' enthält also nur in der r^{ten} Horizontalreihe und in der r^{ten} Verticalreihe Elemente, die von den bezüglichen Elementen z_{gk} verschieden sind.

IV. Aus der Composition von Systemen:

$$\left(a_{ik}^{(-1)}\right)\left(b_{ik}^{(t)}\right)\left(a_{ik}^{(-t)}\right)\left(z_{ik}\right)\left(b_{ik}^{(-t)}\right)\left(a_{ik}^{(t)}\right)\left(b_{ik}^{(-t)}\right)$$

resultirt ein System $\left(z_{ik}^{(r)}\right)$, für welches:

$$z_{11}^{(r)} = z_{rr},\quad z_{rr}^{(r)} = z_{11},\quad z_{rk}^{(r)} = z_{1k},\quad z_{1k}^{(r)} = -z_{rk} \qquad (k=2,\ 3,\ \ldots r-1,\ r+1,\ \ldots n),$$

$$z_{ik}^{(r)} = z_{ik} \qquad (i,\ k=2,\ 3,\ \ldots r-1,\ r+1,\ \ldots n)$$

ist. Das componirte System $\left(z_{ik}^{(r)}\right)$ entsteht also aus dem ursprünglichen System $\left(z_{ik}\right)$, indem darin die erste und r^{te} Horizontalreihe, sowie die erste und r^{te} Verticalreihe mit einander vertauscht, und nach jeder Vertauschung die Zeichen sämmtlicher Elemente der ersten Reihe verändert werden.

V. Ist, wie von jetzt ab vorausgesetzt werden soll, die Determinante des Systems $\left(z_{ik}\right)$ von Null verschieden, so können nicht alle Elemente der ersten Horizontalreihe gleich Null sein. Wenn nun z_{1r} das erste von Null verschiedene Element ist, so kann t so gewählt werden, dass:

$$z_{11} + 2tz_{1r} + t^2 z_{rr} \gtrless 0$$

wird. Man kann also von einem beliebigen symmetrischen Systeme $\left(z_{ik}\right)$ ausgehend, gemäss (II) stets zu einem componirten gelangen, in welchem das neue Element z_{11} von Null verschieden ist.

Ist nun in diesem System, unter den auf z_{11} folgenden Elementen der ersten Horizontalreihe, z_{1r} das erste von Null verschiedene, so kann man gemäss (III) ein System $\left(z_{ik}''\right)$ erhalten, in welchem:

$$z_{1r}'' = z_{1r} + tz_{11},$$

also, wenn man:

$$t = -\frac{z_{1r}}{z_{11}}$$

setzt, $z_{1r}'' = 0$ wird, während die Elemente z_{12}'', z_{13}'', $\ldots$ $z_{1,\,r-1}''$ ebenfalls gleich Null sind, da deren Werthe mit den gleich Null vorausgesetzten Werthen z_{12}, z_{13}, $\ldots$ $z_{1,\,r-1}$ übereinstimmen.

Durch wiederholte Anwendung der hier auseinandergesetzten Methode kann offenbar ein System erlangt werden, in welchem alle Elemente der ersten Horizontal- und Vertical-Reihe mit Ausnahme von z_{11} gleich Null sind. Ein solches System geht ferner, wenn man die in Nr. IV angegebene Composition benutzt, indem man dort $r = n$ nimmt, in ein symmetrisches System über, dessen *letzte* Horizontal- und Vertical-Reihe, mit einziger Ausnahme des Elementes z_{nn}, lauter Nullen enthält.

VI. Setzt man das in Nr. V entwickelte Verfahren fort, so gelangt man schliesslich zu einem Systeme $\left(d_{ik}\right)$, dessen sämmtliche Elemente, mit Ausnahme der in der Diagonale stehenden, gleich Null sind, in welchem also für $i \gtrless k$ stets $d_{ik} = 0$ ist. Ein solches System ergiebt sich demnach aus der Composition einer Reihe von Systemen, in welcher zu beiden Seiten des ursprünglichen Systems $\left(z_{ik}\right)$ lauter Systeme $\left(a_{ik}^{(t)}\right)$, $\left(b_{ik}^{(t)}\right)$ stehen, und zwar in

solcher Aufeinanderfolge, dass je eines der beiden gleich weit von dem mittleren Systeme (z_{ik}) abstehenden das transponirte des anderen ist. Dies kann durch die (symbolische) Compositions-Gleichung:

$$\left(b_{ik}^{(t')}\right) \cdots \left(a_{ik}^{(t)}\right) \cdots \left(z_{ik}\right) \cdots \left(b_{ik}^{(t)}\right) \cdots \left(a_{ik}^{(t')}\right) = \left(d_{ik}\right)$$

angedeutet werden.

VII. Je zwei Systeme $\left(a_{ik}^{(t)}\right)$, $\left(a_{ik}^{(-t)}\right)$ und auch je zwei Systeme $\left(b_{ik}^{(t)}\right)$, $\left(b_{ik}^{(-t)}\right)$ sind zu einander *reciprok*, d. h. sowohl aus der Composition:

$$\left(a_{ik}^{(t)}\right)\left(a_{ik}^{(-t)}\right)$$

als auch aus der Composition:

$$\left(b_{ik}^{(t)}\right)\left(b_{ik}^{(-t)}\right)$$

geht das „*Einheitssystem*“:

$$\left(\delta_{ik}\right)$$

hervor, in welchem $\delta_{ik} = 0$ oder $\delta_{ik} = 1$ ist, je nachdem die beiden Indices von einander verschieden oder einander gleich sind.*) Es bestehen also die (symbolischen) Compositions-Gleichungen:

$$\left(a_{ik}^{(t)}\right)\left(a_{ik}^{(-t)}\right) = \left(\delta_{ik}\right), \quad \left(b_{ik}^{(t)}\right)\left(b_{ik}^{(-t)}\right) = \left(\delta_{ik}\right),$$

und aus der oben in Nr. VI aufgestellten Compositions-Gleichung resultirt daher die folgende:

$$\cdots \left(a_{ik}^{(t)}\right) \cdots \left(z_{ik}\right) \cdots \left(b_{ik}^{(t)}\right) \cdots = \left(b_{ik}^{(-t')}\right)\left(d_{ik}\right)\left(a_{ik}^{(-t')}\right),$$

*) Vergl. meine Notiz „die Subdeterminanten symmetrischer Systeme“ im Sitzungsbericht 1882, XXXVIII[1]), wo ich die oben angewandten Bezeichnungen „reciprok“ und „Einheitssystem“ eingeführt habe.

[1]) Band II S. 389—396 dieser Ausgabe; s. S. 391.

deren linke Seite sich von derjenigen der Gleichung in Nr. VI nur dadurch unterscheidet, dass hier die zwei Systeme fehlen, die dort auf der linken Seite am Anfang und am Ende stehen.

Man kann nun wiederum in derselben Weise die Reihe der Systeme auf der linken Seite dieser neuen Compositions-Gleichung von den beiden am Anfang und am Ende stehenden Systemen befreien, und indem man so fortfährt, gelangt man schliesslich zu einer Gleichung:

$$\left(z_{ik}\right) = \cdots \left(a_{ik}^{(-t)}\right) \cdots \left(b_{ik}^{(-t')}\right)\left(d_{ik}\right)\left(a_{ik}^{(-t')}\right) \cdots \left(b_{ik}^{(-t)}\right) \cdots,$$

welche zeigt:

> dass das ursprüngliche System (z_{ik}) selbst, d. h. also jedes beliebige symmetrische System sich als Resultat der Composition einer Reihe von Systemen darstellen lässt, von denen das mittlere ein System (d_{ik}) ist, während die übrigen, zu beiden Seiten des mittleren, lauter Systeme $\left(a_{ik}^{(t)}\right)$, $\left(b_{ik}^{(t)}\right)$ sind, und zwar in solcher Aufeinanderfolge, dass je eines der beiden von dem mittleren Systeme gleich weit abstehenden das transponirte des andern ist.

Hierbei kann noch angenommen werden, dass die Diagonalelemente d_{kk} des mittleren Systems ihrer Grösse nach auf einander folgen, d. h. also, dass darin für $i < k$ stets $d_{ii} \leqq d_{kk}$ ist; denn die zu solcher Anordnung etwa erforderliche Vertauschung der Diagonalelemente kann durch Composition mit Systemen $\left(a_{ik}^{(1)}\right)$, $\left(a_{ik}^{(-1)}\right)$, $\left(b_{ik}^{(1)}\right)$, $\left(b_{ik}^{(-1)}\right)$ auf die in Nr. IV angegebene Weise bewirkt werden.

VIII. Bezeichnet man zur Abkürzung die Determinante des Systems (z_{ik}) mit Z_s und in analoger Weise die Hauptsubdeterminante:

$$\left| z_{\varrho\lambda} \right| \qquad (\varrho, \lambda = m, m+1, \ldots s)$$

mit Z_m, so ist:

$$Z_2 = \frac{\partial Z_1}{\partial z_{11}}, \quad Z_3 = \frac{\partial Z_2}{\partial z_{22}} = \frac{\partial^2 Z_1}{\partial z_{11} \partial z_{22}}, \cdots Z_n = z_{nn}.$$

Bildet man nun aus dem Systeme (z_{ik}) ein neues: (z'_{ik}), indem man die zweite Horizontalreihe mit Z_3 multiplicirt und zu derselben die dritte, mit $\frac{\partial Z_2}{\partial z_{32}}$ multiplicirt, die vierte mit $\frac{\partial Z_2}{\partial z_{42}}$ multiplicirt u. s. f. addirt, d. h. also, indem man:

$$z'_{1k} = z_{1k}, \quad z'_{2k} = \sum_{g=2}^{g=n} z_{gk} \frac{\partial Z_2}{\partial z_{g2}}, \quad z'_{3k} = z_{3k}, \cdots z'_{nk} = z_{nk}, \qquad (k=1, 2, \ldots n)$$

setzt, so sind die sämmtlichen Elemente z'_{2k} ausser z_{21} durch Z_2 theilbar. Bildet man ferner aus dem Systeme (z'_{ik}) wiederum ein neues: (z''_{ik}), indem man die zweite Verticalreihe mit Z_3 multiplicirt und zu derselben die dritte, mit $\frac{\partial Z_2}{\partial z_{32}}$ multiplicirt, die vierte mit $\frac{\partial Z_2}{\partial z_{42}}$ multiplicirt, u. s. f. addirt, d. h. indem man:

$$z''_{i1} = z'_{i1}, \quad z''_{i2} = \sum_{h=2}^{h=n} z'_{ih} \frac{\partial Z_2}{\partial z_{2h}}, \quad z''_{i3} = z'_{i3}, \cdots z''_{in} = z'_{in} \qquad (i=1, 2, \ldots n)$$

setzt, so ist das System (z''_{ik}) ein *symmetrisches*, und es sind darin alle Elemente, für welche einer der beiden Indices gleich 2 ist, ausser $z''_{12} = z''_{21}$ durch Z_2 theilbar. Ueberdies ist:

$$z''_{ef} = z_{ef} \qquad (e, f=3, 4, \ldots n),$$

und also:

$$|z''_{ik}| \equiv -(z''_{12})^2 |z_{ef}| \pmod{Z_2} \qquad \begin{pmatrix} i, k=1, 2, \ldots n \\ e, f=3, 4, \ldots n \end{pmatrix}.$$

Da nun andererseits offenbar:

$$|z''_{ik}| = Z_3^2 Z_1 \qquad (i, k=1, 2, \ldots n)$$

ist, so resultirt die Congruenz:

$$Z_1 Z_3 \equiv -(z''_{12})^2 \pmod{Z_2},$$

deren Inhalt allgemeiner dahin formulirt werden kann,

> dass *modulo* irgend einer Hauptsubdeterminante eines symmetrischen Systems das Product der beiden benachbarten, für welche die Ordnung der einen um eine Einheit kleiner, die der anderen um eine Einheit grösser ist, stets einem negativen Quadrat congruent wird.

Man kann dasselbe Resultat offenbar aus dem *Jacobi*'schen Hauptsatz über die Subdeterminanten*) erschliessen, und zwar speciell aus der daraus folgenden Determinantenformel:

$$Z_1 Z_3 = -\left(\frac{\partial Z_1}{\partial z_{12}}\right)^2 + Z_2 \frac{\partial Z_1}{\partial z_{22}},$$

aber ich habe hier die obige Herleitung vorgezogen, um die dabei gebrauchte Methode darzulegen.

Nach diesen Vorbereitungen soll nun gezeigt werden,

> dass die $\left(\frac{1}{2}n(n+1)-1\right)$-fache Determinanten-Mannigfaltigkeit $Z_1 = 0$ die gesammte $\frac{1}{2}n(n+1)$-fache Mannigfaltigkeit (z_{ik}) in $n+1$ zusammenhängende Gebiete scheidet, deren jedes durch einen darin liegenden „Hauptpunkt" charakterisirt werden kann, nämlich durch einen solchen, für welchen die ersten v Diagonalelemente z_{kk} gleich -1, die folgenden gleich $+1$ und alle übrigen Elemente z_{ik} gleich Null sind.

Die Anzahl der Hauptpunkte, welche sich ja nur durch die verschiedenen Werthe $v = 0, 1, 2, \cdots n$ von einander unterscheiden, ist gleich $n+1$, also ebenso gross wie die Anzahl der zu charakterisirenden Gebiete.

---

*) Vergl. meine schon oben citirte Notiz im Sitzungsbericht 1882.

§ 1.

Es ist in Nr. VII dargethan worden, dass jedes symmetrische System als Resultat der Composition von Systemen $(a_{ik}^{(0)})$, $(b_{ik}^{(0)})$ mit einem „Diagonalsystem“ (d_{ik}) dargestellt werden kann, in welchem für $i<k$ stets $d_{ii} \leqq d_{kk}$ ist. Sind nun für ein bestimmtes symmetrisches System (ζ_{ik}) die Werthe der Elemente t in den verschiedenen Componenten-Systemen der Reihe nach:

$$\tau_1,\ \tau_2,\ \tau_3, \ldots,$$

so resultirt, wenn an deren Stelle variable Grössen:

$$t_1,\ t_2,\ t_3, \ldots$$

gesetzt werden, ein symmetrisches System mit variabeln Elementen (z_{ik}). Lässt man jetzt t_1 von τ_1 bis 0, ferner t_2 von τ_2 bis 0 u. s. f. variiren, so geht das System (ζ_{ik}) in das System (d_{ik}) continuirlich über, und zwar ohne dass die Determinante ihren Werth ändert.

In dem Systeme (d_{ik}) kann ferner jedes der negativen Diagonalelemente in -1 und jedes der positiven Diagonalelemente in $+1$ continuirlich übergeführt werden, ohne dass dabei die Determinante gleich Null wird.

Man kann also von jedem Punkte (ζ_{ik}) der $\frac{1}{2}n(n+1)$-fachen Mannigfaltigkeit (z_{ik}), ohne die Determinanten-Mannigfaltigkeit zu passiren, zu einem „Hauptpunkte“ gelangen, d. h. zu einem solchen, für den:

$$z_{11} = z_{22} = \cdots = z_{\nu\nu} = -1\,; \quad z_{\nu+1,\,\nu+1} = \cdots = z_{nn} = +1$$

ist und alle übrigen Elemente z_{ik} gleich Null sind.

In jedem der Gebiete, welche durch die Determinanten-Mannigfaltigkeit $Z_\nu = 0$ von einander geschieden werden, muss daher wenigstens *einer* der Hauptpunkte liegen, und es soll nun im folgenden Paragraphen gezeigt werden, dass in der That *nur* einer darin liegt.

§ 2.

Um den angekündigten Nachweis führen zu können, muss zuvörderst die Veränderung untersucht werden, welche der Werth der Summe:

$$(S) \qquad \operatorname{sgn.} Z_1 Z_2 + \operatorname{sgn.} Z_2 Z_3 + \cdots + \operatorname{sgn.} Z_{n-1} Z_n + \operatorname{sgn.} Z_n$$

bei Variirung des symmetrischen Systems (z_{ik}) erleidet.*) Dabei möge der Werth dieser Summe, als Function des symmetrischen Systems (z_{ik}) oder des „Punktes“ (z_{ik}), zur Abkürzung mit:

$$S((z_{ik}))$$

bezeichnet werden.

Geht man von einem bestimmten Punkte (ζ_{ik}) zu einem benachbarten (ζ'_{ik}) über, d. h. lässt man das System (z_{ik}) von einem bestimmten Systeme (ζ_{ik}) bis zu einem benachbarten (ζ'_{ik}) stetig variiren, so bleibt der Werth der Summe sicher ungeändert, wenn sich dabei keines der Zeichen:

$$\operatorname{sgn.} Z_m \qquad (m=1, 2, \ldots n)$$

ändert. Der Werth der Summe kann sich also nur dann ändern, wenn man eine der $\left(\frac{1}{2}n(n+1)-1\right)$-fachen Mannigfaltigkeiten:

$$Z_m = 0 \qquad (m=1, 2, \ldots n)$$

passirt, und zwar an einer Stelle, wo Z_m aus dem Positiven ins Negative oder umgekehrt übergeht. Es ist daher bloss zu untersuchen, ob ein solcher Durchgang durch eine dieser Mannigfaltigkeiten eine Aenderung des Werthes der Summe (S) bewirkt.

Demgemäss sei sgn. Z_m im Punkte (ζ_{ik}) negativ und im Punkte (ζ'_{ik}) positiv; ferner sei (ζ^0_{ik}) der auf dem Wege von (ζ_{ik}) zu (ζ'_{ik}) passirte Punkt

*) Vergl. *Hazzidakis*: Ueber eine Eigenschaft der Unterdeterminanten einer symmetrischen Determinante. Journal f. Math. Bd. 91.

der Mannigfaltigkeit $Z_m = 0$. Sollte nun der Punkt (ξ_{ik}^0) zugleich auf einer oder mehreren der anderen Mannigfaltigkeiten:

$$\cdots Z_{m-2} = 0, \quad Z_{m-1} = 0, \quad Z_{m+1} = 0, \quad Z_{m+2} = 0, \cdots$$

liegen, so kann man zu einem auf der Mannigfaltigkeit $Z_m = 0$ liegenden benachbarten Punkte $(\overline{\xi}_{ik}^0)$ übergehen, für welchen jeder der anderen Werthe $\ldots Z_{m-1}, Z_{m+1}, \ldots$ von Null verschieden ist. Bezeichnet man diese Werthe beziehungsweise mit $\ldots W_{m-1}, W_{m+1}, \ldots$, so liegt der Punkt $(\overline{\xi}_{ik}^0)$ der Mannigfaltigkeit $Z_m = 0$ zugleich auf den Mannigfaltigkeiten:

$$\cdots Z_{m-1} = W_{m-1}, \quad Z_{m+1} = W_{m+1}, \cdots,$$

und man kann weiter, auf diesen Mannigfaltigkeiten bleibend, einerseits zu einem benachbarten Punkte $(\overline{\xi}_{ik})$ übergehen, für welchen $Z_m < 0$ ist, und andererseits zu einem benachbarten Punkte $(\overline{\xi}_{ik}')$, für welchen $Z_m > 0$ ist. Endlich kann man einerseits vom Punkte $(\overline{\xi}_{ik})$ zu (ξ_{ik}) und andererseits vom Punkte $(\overline{\xi}_{ik}')$ zu (ξ_{ik}') so gelangen, dass Z_m in dem einen Falle durchweg negativ, in dem anderen durchweg positiv bleibt. Anstatt des Uebergangs auf dem Wege:

$$(\xi_{ik}), \quad (\xi_{ik}^0), \quad (\xi_{ik})$$

kann also der Uebergang auf dem Wege:

$$(\xi_{ik}), \quad (\overline{\xi}_{ik}), \quad (\overline{\xi}_{ik}^0), \quad (\overline{\xi}_{ik}'), \quad (\xi_{ik}')$$

geschehen, bei welchem die Mannigfaltigkeit $Z_m = 0$ an einer Stelle überschritten wird, wo jeder der anderen Werthe $\ldots Z_{m-1}, Z_{m+1}, \ldots$ von Null verschieden ist.

Die vorstehende Deduction gilt, natürlich mit Weglassung von Z_{m-1}, auch für den Fall $m = 1$, und man sieht daher, dass nur zu untersuchen ist,

> ob der Durchgang durch eine der Mannigfaltigkeiten $Z_m = 0$ an einer Stelle, wo eine Determinante Z_m ihr Zeichen wechselt und alle übrigen Determinanten von Null verschiedene Werthe haben, eine Aenderung des Werthes der Summe (S) bewirkt.

Es ist nun klar, dass bei einem derartigen Durchgang durch die Determinanten-Mannigfaltigkeit $Z_1 = 0$ der Werth der Summe (S) sich um zwei Einheiten ändert, da das erste Glied:

$$\text{sgn. } Z_1 Z_2$$

eine solche Aenderung erfährt, alle übrigen Glieder aber ihren Werth beibehalten.

Aber beim Durchgang durch eine der *Subdeterminanten*-Mannigfaltigkeiten $Z_2 = 0, Z_3 = 0, \cdots, Z_n = 0$ erfolgt keine Aenderung des Werthes der Summe (S). Denn für jeden der Werthe:

$$m = 2, 3, \cdots n-1$$

wird, wie oben in Nr. VIII gezeigt worden ist:

$$Z_{m-1} Z_{m+1} \quad \textit{modulo } Z_m$$

einem negativen Quadrate congruent; für $Z_m = 0$ ist daher, wenn, wie es bei dem Durchgang durch $Z_m = 0$ der Fall ist, die Werthe von Z_{m-1} und Z_{m+1} von Null verschieden sind:

$$\text{sgn. } Z_{m-1} = -\text{ sgn. } Z_{m+1},$$

und da dieselbe Relation für die beiden dem Durchgangspunkt benachbarten Punkte (ξ_{ik}), (ξ_{ik}') besteht, während Z_m für (ξ_{ik}) positiv, für (ξ_{ik}') negativ ist, so ist für beide Punkte, so wie für alle diejenigen, welche auf dem Wege von (ξ_{ik}) zu (ξ_{ik}') passirt werden:

$$\text{sgn. } Z_{m-1} Z_m + \text{sgn. } Z_m Z_{m+1} = 0.$$

Das Aggregat dieser beiden Glieder erfährt also bei jenem Durchgang durch $Z_m = 0$ keinerlei Werthänderung, und die übrigen Glieder der Summe bleiben dabei ebenfalls ungeändert, da alle anderen Subdeterminanten ihre Zeichen beibehalten.

Alles dies gilt auch für $m = n$, wenn man $Z_{n+1} = 1$ setzt, da alsdann die Congruenz:

$$Z_{n-1} Z_{n+1} \equiv -(z_{n-1,\,n})^2 \pmod{Z_n}$$

besteht und an diese die obigen Schlussfolgerungen geknüpft werden können.

Das Resultat der vorstehenden Auseinandersetzung kann dahin formulirt werden:

> Der Werth von $S((z_{ik}))$ ändert sich nur dann, wenn der Punkt durch die Determinanten-Mannigfaltigkeit $Z_1 = 0$ hindurchgeht, und zwar genau um zwei Einheiten, wenn der Durchgang an einer nicht singulären Stelle erfolgt.

Nun wird für einen Hauptpunkt (z_{ik}), für welchen:

$$z_{11} = z_{22} = \cdots = z_{\nu\nu} = -1; \quad z_{\nu+1,\,\nu+1} = \cdots = z_{nn} = +1$$

ist:

$$Z_1 = (-1)^\nu, \quad Z_2 = (-1)^{\nu-1}, \cdots Z_\nu = (-1); \quad Z_{\nu+1} = \cdots = Z_n = 1,$$

und also:

$$S((z_{ik})) = n - 2\nu.$$

Für jeden der $n+1$ Hauptpunkte, welchen die $n+1$ verschiedenen Werthe $\nu = 0, 1, 2, \cdots n$ entsprechen, hat daher $S((z_{ik}))$ einen andern Werth, und es folgt hieraus,

> dass es *nicht* möglich ist, von einem Hauptpunkte zu einem andern zu kommen, ohne die Determinanten-Mannigfaltigkeit $Z_1 = 0$ zu passiren, d. h., dass die verschiedenen Hauptpunkte in verschiedenen Gebieten liegen und diese also vollständig charakterisiren.

Hiermit ist der am Schlusse des § 1 angekündigte Nachweis geführt, und die Angaben, welche über die Gebietstheilung durch die Determinanten-Mannigfaltigkeit unmittelbar vor § 1 gemacht worden sind, haben nunmehr sämmtlich ihre Bestätigung gefunden.

§ 3.

Für ein nicht symmetrisches aus n^2 unabhängigen Veränderlichen bestehendes System (y_{ik}) kann die Frage der Gebietstheilung der n^2-fachen Mannigfaltigkeit:

$$y_{ik} \qquad (i, k = 1, 2, \ldots n)$$

durch die (n^2-1)-fache Mannigfaltigkeit:

$$|y_{ik}| = 0 \qquad (i, k = 1, 2, \ldots n)$$

in ähnlicher, aber einfacherer Weise erledigt werden.

Zu diesem Zwecke soll zuvörderst gezeigt werden, wie sich ein solches System (y_{ik}) als Resultat der Composition gewisser einfacher Systeme darstellen lässt.

Erstens resultirt aus der Composition:

$$(a_{ik}^{(0)})\ (y_{ik})$$

ein System (y_{ik}^0), in welchem:

$$y_{1k}^{(0)} = y_{1k} + t y_{rk}\,, \quad y_{ik}^0 = y_{ik} \qquad \begin{pmatrix} i = 2, 3, \ldots n \\ k = 1, 2, 3, \ldots n \end{pmatrix}$$

ist, während aus der Composition:

$$(y_{ik})\,(a_{ik}^{(\sigma)})$$

ein System (y'_{ik}) hervorgeht, in welchem:

$$y'_{ir} = ty_{i1} + y_{ir}, \quad y'_{ik} = y_{ik} \qquad \begin{pmatrix} i=1,2,\dots n \\ k=1,2,\dots r-1,\ r+1,\dots n \end{pmatrix}$$

ist.

Zweitens entsteht aus der Composition der Systeme:

$$(a_{ik}^{(-1)})\,(b_{ik}^{(1)})\,(a_{ik}^{(-1)})\,(y_{ik})$$

ein System $y_{ik}^{(\delta)}$, für welches:

$$y_{1k}^{(\delta)} = -y_{rk}, \quad y_{rk}^{(\delta)} = y_{1k}, \quad y_{ik}^{(\delta)} = y_{ik} \qquad \begin{pmatrix} k=1,2,\dots n \\ i=2,3,\dots r-1,\ r+1,\dots n \end{pmatrix}$$

ist, so dass in dem componirten System die erste und r^{te} Horizontalreihe des ursprünglichen Systems mit einander vertauscht und überdies die Zeichen der neuen ersten Horizontalreihe verändert sind.

Drittens resultirt aus der Composition der Systeme:

$$(y_{ik})\,(a_{ik}^{(-1)})\,(b_{ik}^{(1)})\,(a_{ik}^{(-1)})$$

ein System $(y_{ik}^{(\sigma)})$, für welches:

$$y_{i1}^{(\sigma)} = y_{ir}, \quad y_{ir}^{(\sigma)} = -y_{i1}, \quad y_{ik}^{(\sigma)} = y_{ik} \qquad \begin{pmatrix} i=1,2,\dots n \\ k=2,3,\dots r-1,\ r+1,\dots n \end{pmatrix}$$

ist, so dass in dem componirten Systeme die erste und r^{te} Verticalreihe des ursprünglichen Systems mit einander vertauscht und überdies die Zeichen der neuen r^{ten} Verticalreihe verändert sind.

Viertens gelangt man bei nochmaliger Anwendung der zuletzt angegebenen Composition zu einem Systeme, welches sich von dem ursprünglichen nur dadurch unterscheidet, dass die Vorzeichen der ersten und der r^{ten} Verticalreihe verändert sind.

Geht man nun von irgend einem bestimmten System (η_{ik}) aus, so kann man, falls $\eta_{11} = 0$ ist, durch Vertauschung von Verticalreihen ein System $(\eta_{ik}^{(\sigma)})$ erhalten, in welchem dies nicht der Fall ist. Alsdann kann man durch Zusammensetzung mit einem System $(a_{ik}^{(\sigma)})$, in welchem:

$$t = -\frac{\eta_{1r}}{\eta_{11}}$$

anzunehmen ist, zu einem System gelangen, in dessen erster Horizontalreihe das r^{te} Element gleich Null ist. Hat man, so fortfahrend, alle Elemente der ersten Horizontalreihe, mit Ausnahme des ersten zum Verschwinden gebracht, so kann man durch Vertauschung der Horizontalreihen die erste an die letzte Stelle bringen und alsdann die angegebene Operation mit derjenigen Horizontalreihe, welche nunmehr die erste ist, wieder beginnen. Durch Wiederholung dieses Verfahrens gelangt man schliesslich zu einem Systeme (d_{ik}), welches nur in der Diagonale von Null verschiedene Elemente enthält.

Componirt man dieses System mit einem anderen $(\mathfrak{d}_{ik})$, dessen Elemente ausserhalb der Diagonale sämmtlich gleich Null und in der Diagonale, mit Ausnahme von $\mathfrak{d}_{11}$, sämmtlich gleich Eins sind, so entsteht ein „Diagonalsystem", welches sich von (d_{ik}) nur dadurch unterscheidet, dass das erste Element gleich dem Product $d_{11}\mathfrak{d}_{11}$ ist. Das erste Element dieses componirten Systems wird also gleich ± 1, wenn $\mathfrak{d}_{11}$ gleich dem reciproken Werthe des absoluten von d_{11} genommen wird. Bringt man dann durch Vertauschung von Horizontal- und Verticalreihen, welche nach Nr. IV durch Composition mit Systemen (a_{ik}), (b_{ik}) zu bewirken ist, jenes erste Element ± 1 an die zweite und d_{22} an die erste Stelle, so kann man nunmehr durch Composition mit einem Systeme $(\mathfrak{d}_{ik})$ zu einem Diagonalsysteme gelangen, in welchem das erste und zweite Element gleich ± 1 ist, und die Fortsetzung dieses Verfahrens führt offenbar zu einem Systeme, in welchem sämmtliche Elemente in der Diagonale gleich ± 1 und alle übrigen gleich Null sind.

Ein solches System kann, wenn ein Element -1 darin vorkommt, durch Vertauschung der Horizontal- und Vertical-Reihen so eingerichtet werden, dass das *erste* Element gleich -1 ist. Dann kann man, wenn noch ein Element -1 vorhanden ist, durch Composition mit Systemen (a_{ik}), (b_{ik}) in der oben (bei „*viertens*“) angegebenen Weise ein anderes System erhalten, in welchem die *beiden* Elemente -1 durch $+1$ ersetzt sind. Durch wiederholte Anwendung dieses Verfahrens gelangt man schliesslich entweder zu dem Einheitssysteme (δ_{ik}) oder aber zu einem Diagonalsysteme (d_{ik}), in welchem:

$$d_{11} = -1, \quad d_{22} = d_{33} = \cdots = d_{nn} = 1$$

ist, und der eine oder der andere Fall tritt ein, je nachdem die Determinante des Systems (η_{ik}), von dem ausgegangen wurde, positiv oder negativ ist.

Aus der vorstehenden Entwickelung folgt,

dass jedes beliebige System (η_{ik}), dessen Determinante positiv ist, sich als Resultat der Composition von Systemen:

$$\left(a_{ik}^{(\varrho)}\right), \quad \left(b_{ik}^{(\alpha)}\right), \quad \left(\mathfrak{b}_{ik}\right)$$

darstellen lässt, während, wenn die Determinante negativ ist, noch am Anfange oder am Ende der Reihe der Componenten-Systeme eines hinzuzufügen ist, welches aus dem Einheitssysteme entsteht, indem für das erste Element an Stelle der positiven die negative *Eins* gesetzt wird.

Dabei möge die Bedeutung der Systeme $\left(a_{ik}^{(\varrho)}\right)$, $\left(b_{ik}^{(\alpha)}\right)$, $\left(\mathfrak{b}_{ik}\right)$ hier nochmals dahin präcisirt werden,

dass erstens jedes System $\left(a_{ik}^{(\varrho)}\right)$ in der Diagonale lauter Elemente $+1$, ferner als r^{tes} Element der ersten Horizontalreihe die Grösse t und im Uebrigen nur Nullen enthält, dass zweitens das System $\left(b_{ik}^{(\alpha)}\right)$ in der Diagonale lauter Elemente $+1$, ferner als r^{tes} Element der ersten Verticalreihe $+1$ und im Uebrigen nur Nullen enthält, dass

drittens in jedem Systeme $(\mathfrak{b}_{ik})$ das erste Element $\mathfrak{b}_{11}$ eine positive Grösse ist, die folgenden Diagonal-Elemente aber gleich $+1$ und alle übrigen Elemente gleich Null sind.

Sind bei der angegebenen Darstellung des Systems (η_{ik}) die Werthe der Elemente t in den verschiedenen Componenten-Systemen (a_{ik}):

$$\tau_1, \ \tau_2, \ \tau_3, \ \ldots,$$

und die positiven Werthe der Elemente $\mathfrak{b}_{11}$ in den Systemen $(\mathfrak{b}_{ik})$:

$$\mathfrak{b}', \ \mathfrak{b}'', \ \mathfrak{b}''', \ \ldots,$$

so resultirt, wenn man $\tau_1, \tau_2, \tau_3, \ldots$ durch variable Grössen:

$$t_1, \ t_2, \ t_3, \ \ldots,$$

ferner die ausserhalb der Diagonale in den Systemen $\left(b_{ik}^{(\alpha)}\right)$ vorkommenden Elemente 1 durch variable Elemente:

$$t_1', \ t_2', \ t_3', \ \ldots$$

und endlich auch jene positiven Elemente $\mathfrak{b}', \mathfrak{b}'', \mathfrak{b}''', \ldots$ durch variable Elemente

$$d', \ d'', \ d''', \ \ldots$$

ersetzt, ein System (y_{ik}) mit variabeln Elementen. Lässt man jetzt t_1 von τ_1 bis 0, ebenso t_2 von τ_2 bis 0, $\ldots$, ferner jede der Variabeln t' von 1 bis 0 und endlich d' von $\mathfrak{b}$ bis 1, d'' von $\mathfrak{b}''$ bis 1 u. s. f. variiren, so geht das System (η_{ik}) entweder in das Einheitssystem (δ_{ik}) oder in das System:

$$\begin{pmatrix} -1, & 0, & 0, & \cdots \\ 0, & 1, & 0, & \cdots \\ 0, & 0, & 1, & \cdots \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix}$$

über, je nachdem die Determinante des Systems (η_{ik}) einen positiven oder negativen Werth hat. Da nun bei jenem Uebergange offenbar kein System (y_{ik}) passirt wird, dessen Determinante gleich Null ist, so ergiebt sich,

dass die n^2-fache Mannigfaltigkeit (y_{ik}) durch die (n^2-1)-fache Mannigfaltigkeit:

$$|y_{ik}| = 0 \qquad (i, k = 1, 2, \ldots n)$$

in nur zwei zusammenhängende Gebiete geschieden wird.

Dabei ist natürlich in dem einen Gebiete der Werth der Determinante positiv, in dem anderen negativ.

DIE DECOMPOSITION DER SYSTEME VON n^2 GRÖSSEN UND IHRE ANWENDUNG AUF DIE THEORIE DER INVARIANTEN.

VON

L. KRONECKER.

Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin vom Jahre 1889. S. 479—505, 603—614.