Ueber einige Bildungsgesetze in der Theorie der Theilung und der Transformation der elliptischen Functionen.

Von

Von G. Morera in Novara.

Die vorliegende Note steht in engem Zusammenhange mit der Abhandlung des Herrn Prof. Klein: „Ueber die Auflösung gewisser Gleichungen vom siebenten und achten Grade", welche im 15ten Bande der Annalen erschienen ist.

Nach den dort*) geschilderten allgemeinen Principien wird die Reduction eines algebraischen Problems auf ein anderes, einfacherer Natur, durch die Bildung gewisser Systeme von neuen Variabeln geleistet, deren charakteristische Eigenschaft ist, bei den Vertauschungen der Galois'schen Gruppe der vorgelegten Gleichung *sich linear homogen in geschlossener Gruppe zu transformiren.*

In derselben Abhandlung ist ein *Fundamentalsatz* gegeben, um solche Systeme aus ihren charakteristischen Eigenschaften wirklich herzustellen (§ 1).

In der nachstehenden Note werden die Bildungsgesetze für einige Systeme gegeben, welche bei der n-Theilung und der Transformation n^{ter} Ordnung der elliptischen Functionen eine wichtige Rolle spielen. Hierbei wird nur der Fall $n =$ *eine ungerade Primzahl* betrachtet.

Diese Bildungsgesetze sind freilich zum Theil bekannt, aber ihre grosse Wichtigkeit für gewisse algebraische Untersuchungen (wie z. B. bei der Theorie der Gleichung vom fünften Grade) lässt mir wünschenswerth scheinen, sie vollständig darzulegen. Uebrigens wolle man insbesondere die Arbeit vergleichen, welche Herr Kronecker in den

*) Vgl. die §§ 2 und 3 der angegebenen Abhandlung, oder auch: Vorlesungen über das Ikosaeder etc. (Leipzig 1884), p 125 ff.

Sitzungsberichten der Berliner Akademie von 1879 veröffentlicht hat (p. 220 ff. Ueber die Classe der Gleichungen, von denen die Theilung der elliptischen Functionen abhängt.)

§ 1.

Es seien $\Phi_{a,b}$, wo a und b die Zahlen 0, 1, 2, 3, ..., $n-1$ mit Ausschluss der Combination $a = b = 0$ durchlaufen dürfen, die $n^2 - 1$ Wurzeln einer algebraischen Gleichung, deren *Galois*'sche Gruppe Γ durch die linearen Substitutionen

$$| a,\ b;\ a\alpha + b\gamma,\ a\beta + b\delta | \ (\text{mod. } n)$$

definirt ist, worin $\alpha, \beta, \gamma, \delta$ ganze Zahlen bezeichnen, die der einzigen Bedingung:

$$\alpha\delta - \beta\gamma \equiv 1 \ (\text{mod. } n)$$

unterworfen sind.

Dies ist die bekannte Monodromiegruppe der speciellen Theilungsgleichung für eine ungerade elliptische Function.

Wir werden die eben hingeschriebene Substitution als *eine Operation* $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ *bezeichnen.*

Solcher Operationen giebt es bekanntlich $n(n^2-1)$*).

Wenn es sich um elliptische Functionen handelt, d. h. wenn die $\Phi_{a,b}$ *Modulformen* sind, so kommt die genannte Operation darauf hinaus, *statt der ursprünglichen Perioden* ω_1, ω_2 *die neuen* $\alpha\omega_1 + \beta\omega_2$, $\gamma\omega_1 + \delta\omega_2$ $(\alpha\delta - \beta\gamma = 1)$ *einzuführen.*

Was die Zusammensetzung dieser Operationen anbelangt, gilt die einfache Regel:

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' + \beta\gamma' & \alpha\beta' + \beta\delta' \\ \gamma\alpha' + \delta\gamma' & \gamma\beta' + \delta\delta' \end{pmatrix}.$$

Die Operationen unserer Gruppe können alle aus den zwei folgenden erzeugt werden:

$$S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix};$$

aber um eine einfache Darstellung der ganzen Gruppe zu gewinnen, ist es zweckmässig die dritte erzeugende Operation einzuführen:

$$U \equiv \begin{pmatrix} g & 0 \\ 0 & \frac{1}{g} \end{pmatrix} \quad (\text{mod. } n),$$

wo g eine Primitivwurzel von n bedeutet.

---

*) Unter n ist, wie schon gesagt, immer eine *ungerade Primzahl* zu verstehen.

§ 2.

Die Operation U hat offenbar die Periode $n-1$ und ihre Potenzen sind, von der Reihenfolge abgesehen:

$$U_a \equiv \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix} \pmod{n}$$

$$(a = 1, 2, 3, \ldots, n-1).$$

Unsere gesammte Gruppe umfasst, wie bekannt, die Operationen:

$$S^k U_a \equiv \begin{pmatrix} a & \frac{k}{a} \\ 0 & \frac{1}{a} \end{pmatrix}; \quad S^k U_a T S^{k'} \equiv \begin{pmatrix} \frac{k}{a} & \frac{kk'}{a} - a \\ \frac{1}{a} & \frac{k'}{a} \end{pmatrix},$$

$$\begin{pmatrix} k, k' = 0, 1, 2, \ldots, n-1 \\ a = 1, 2, 3, \ldots, n-1 \end{pmatrix}.$$

So ist unsere Gruppe durch drei Operationen: S, T, U vollständig erzeugt.

Die Operation U_a ist natürlich ihrerseits durch die Grundoperationen S und T darstellbar.

Man hat zunächst:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{l} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{l'} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{l''} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{l'''}$$

$$= \begin{pmatrix} 1 + ll' + l''[l + l''(1 + ll')] & l + l''(1 + ll') \\ l' + l''(1 + l'l') & 1 + l'l'' \end{pmatrix}.$$

Um diesen Ausdruck mit U_a zur Uebereinstimmung zu bringen, braucht man nur

$$l \equiv -\frac{a(a-1)}{l'''}, \quad l' \equiv -\frac{l'''}{a}, \quad l'' \equiv \frac{a-1}{l'''} \pmod{n}$$

zu setzen. Es ist aber

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = STS,$$

also:

$$U_a \equiv S^{-\frac{a(a-1)}{l'''}} \cdot (STS)^{-\frac{l'''}{a}} \cdot S^{\frac{a-1}{l'''}} (STS)^{l'''},$$

wo l''' eine noch unbestimmte Zahl bedeutet.

Indem man beachtet, dass

$$(STS)^a = TS^{-a}T^{-1}$$

und für $l''' : \pm a$ annimmt, bekommt man:

$$U_a = S^{-a} . T^{-1} . S^{-\frac{1}{a}} . T . S^{-a} . T^{-1}$$
$$= S^{a} . T \quad . S^{\frac{1}{a}} \quad . T . S^{a} \quad . T^{-1}.$$

Ich stelle noch folgende Formeln zusammen, die man leicht beweist:

$$\begin{cases} U_l . T = T . U_{\frac{1}{l}} ; \\ S^k . U_l = U_l . S^{\frac{k}{l^2}} ; \\ T . S^k . U_l = U_{\frac{1}{l}} . T . S^{\frac{k}{l^2}} ; \\ S^k . U_l . T . S^{k'} . T = S^{k-\frac{l^2}{k'}} . U_{\frac{l}{k'}} . T . S^{\frac{1}{k'}} ; \\ T^2 = U_{-1} ; \\ T . S^k . T = S^{-\frac{1}{k}} . U_{\frac{1}{k}} . T . S^{-\frac{1}{k}} . \end{cases}$$

§ 3.

Vermöge der vorausgeschickten Formeln erkennt man leicht die Richtigkeit folgenden Theorems:

Will man aus einem gegebenen Φ-Systeme die allgemeinsten Φ bilden, so kann man folgendermassen verfahren. Man bildet irgend welche rationale Function G der gegebenen Elemente, welche bei den Operationen der Gruppe S^k ($k = 0, 1, 2, \ldots, n-1$) und nur bei diesen unverändert bleibt. Dann hat man:

$$\Phi_{0,l} = (G)\, U_{\frac{1}{l}} ; \qquad \Phi_{l,lk} = (G)\, U_{\frac{1}{l}}\, T\, S^k .$$

Für die Elemente $\Phi_{a,b}$ haben wir die wohl bekannte Eintheilung in $n+1$ Reihen:

$$\begin{cases} \Phi_{0,g^0}, & \Phi_{0,g}, & \Phi_{0,g^2}, & \ldots \Phi_{0,g^{n-2}} ; & (\infty); \\ \Phi_{g^0,0}, & \Phi_{g,0}, & \Phi_{g^3,g}, & \ldots \Phi_{g^{n-2},0} ; & (0); \\ \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \\ \Phi_{g^0,g^0\nu}, & \Phi_{g,g\nu}, & \Phi_{g^2,g^2\nu}, & \ldots \Phi_{g^{n-2},g^{n-2}\nu} ; & (\nu); \\ \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \\ \Phi_{g^0,g^0(n-1)}, & \Phi_{g,g(n-1)}, & \Phi_{g^2,g^3(n-1)}, & \ldots \Phi_{g^{n-2},g^{n-2}(n-1)} ; & (n-1), \end{cases}$$

wo g eine Primitivwurzel von n bezeichnet. Nun hat diesbezüglich die Gruppe Γ bekanntlich folgende Eigenschaften:

1) Die Reihen $(\infty), (0), (1), \ldots, (n-1)$ werden unter einander vertauscht, wie die Wurzeln der Modulargleichung bei ihrer Monodromiegruppe.

2) Die Elemente jeder Reihe werden gleichzeitig unter einander cyklisch vertauscht.

Hieraus fliesst ohne Weiteres das Theorem:

Will man mit einem Φ-Systeme ein System von $n+1$ Variabeln: $C_\infty, C_0, C_1 \ldots C_{n-1}$ aufbauen, welche den Vertauschungen der Monodromiegruppe der Modulargleichung unterworfen sein sollen, so braucht man nur eine metacyklische Function M zu bilden, d. h. eine Function, die bei den Vertauschungen der Gruppe

$$S^k \cdot U_l \quad (k = 0, 1, 2 \ldots n-1;\ l = 1, 2 \ldots n-1)$$

und nur bei diesen unverändert bleibt. Man hat dann:

$$C_\infty = M, \quad C_0 = (M)\,T, \ldots, C_\nu = (M)\,T \cdot S^\nu \ldots .$$

§ 4.

Wir werden jetzt Systeme von Variabeln untersuchen, welche nicht mehr bloss unter einander vertauscht werden, sondern *lineare homogene Substitutionen erfahren.*

Dabei wollen wir folgende Bemerkung voranschicken.

Wenn man bei einer linear homogenen Substitutionsgruppe unter p Variabeln, p particuläre unter einander unabhängige Systeme der gewünschten Eigenschaft gefunden hat, dann *können alle anderen durch diese linear homogen mit invarianten Coefficienten zusammengesetzt werden**).

Also ist die Frage immer als gelöst zu betrachten, wenn einmal diese besonderen Systeme wirklich aufgebaut sind.

Wir betrachten zunächst eine Substitutionsgruppe bei $n+1$ Variabeln

$$D_\infty, D_0, D_1, \ldots, D_{n-1},$$

die man folgendermassen definirt hat:

$$\begin{cases} (D_\mu)\ S = D_{\mu+1}; \quad (\mu = \infty, 0, 1, \ldots, n-1), \\ (D_\infty)\ T = D_0; \quad (D_0)\ T = \binom{-1}{n} D_\infty; \quad (D_l)\ T = \binom{l}{n} D_{\frac{1}{l}}; \\ \qquad\qquad (l = 1, 2, 3, \ldots, n-1), \\ D_\mu U_a = \binom{a}{n} D_{\frac{\mu}{a^2}}. \end{cases}$$

*) Man sehe auch Klein, Vorlesungen über das Ikosaeder etc., pag. 227 ff.

Diese Operationsgruppe ist mit der Gruppe Γ *holoedrisch isomorph, wenn* $\left(\frac{-1}{n}\right) = -1$, *d. h. wenn:* $n \equiv -1$ (*mod.* 4). *Wenn dagegen:* $n \equiv +1$ (*mod.* 4), *so ist der Isomorphismus hemiedrisch*, d. h. die Operationen der Gruppe sind nur in der Zahl $\frac{n(n^2-1)}{2}$ vorhanden.

Für das Bildungsgesetz dieser Variabeln giebt der erwähnte Fundamentalsatz die folgende Regel:

Man bilde mit den Φ *eine halbmetacyclische Function* H, *d. h. eine Function, die bloss bei den Substitutionen der Gruppe* $S_k U_R$ (*wo* R *alle quadratischen Reste* (*mod.* n) *und* k *die Zahlen* $0, 1, 2 \ldots n-1$ *durchläuft*) *ungeändert bleibt, und es sei* H' *der aus* H *erhaltene Werth, wenn auf* H *eine Operation* U_N (*wo* N *einen Nichtrest bezeichnet*) *angewandt wird. Dann hat man:*

$$D_\infty = H - H',$$
$$D_k = [H - H'] TS^k.$$

Wenn man die Function H insbesondere aus den Elementen der Reihe (∞) in der oben angeführten Eintheilung der Variabeln Φ zusammensetzt, so hat man folgendes Bildungsgesetz, welches schon von Hrn. Kronecker in den Berliner Monatsberichten aus dem Jahre 1879 (l. c.) gegeben worden ist:

Man bilde aus jeder Reihe eine cyklische Function der Elemente, deren erste Indices Reste sind, nämlich von den Elementen:

$$\Phi_{0,g^0}, \quad \Phi_{0,g^2}, \quad \Phi_{0,g^4}, \quad \ldots \quad \Phi_{0,g^{n-3}} \qquad \text{für die Reihe } (\infty);$$

und den Elementen:

$$\Phi_{g^0,g^0\nu}, \quad \Phi_{g^2,g^2\nu}, \quad \Phi_{g^4,g^4\nu}, \quad \ldots \quad \Phi_{g^{n-3},g^{n-3}\nu} \text{ für die Reihe } (\nu).$$

Wir nennen diese Functionen bez. S_∞ und S_ν. Man bilde ferner für jede Reihe dieselben Functionen mit den Elementen, deren Indices Nichtreste sind, nämlich mit den Elementen:

$$\Phi_{0,g}, \quad \Phi_{0,g^3}, \quad \Phi_{0,g^5}, \quad \ldots \quad \Phi_{0,g^{n-2}} \qquad \text{für die Reihe } (\infty);$$

und den Elementen

$$\Phi_{g,g\nu}, \quad \Phi_{g^3,g^3\nu}, \quad \Phi_{g^5,g^5\nu}, \quad \ldots \quad \Phi_{g^{n-2},g^{n-2}} \text{ für die Reihe } (\nu);$$

wir nennen dieselben bez. S'_∞, S'_ν. Dann hat man:

$$D_\infty = S_\infty - S'_\infty;$$
$$D_\nu = S_\nu - S'_\nu.$$

Hat man ein besonderes $\overline{D}$-System gefunden, so sind alle Anderen, wie Hr. Kronecker bemerkt, durch die Formeln:

$$D_\infty = \lambda D_\infty + \lambda_1 D_\infty^{\,3} + \cdots + \lambda_n D_\infty^{\,2n+1};$$
$$D_k = \lambda D_k + \lambda_1 D_k^{\,3} + \cdots + \lambda_n D_k^{\,2n+1},$$

dargestellt, wo $\lambda, \lambda_1, \ldots, \lambda_n$ invariante Coefficienten sind. Die geraden Potenzen der Variabeln D sind offenbar Variabeln C; man vergl. den Schlusssatz des vorigen Paragraphen.

§ 5.

Bei $\frac{n+1}{2}$ Variabeln

$$A_0, A_1, A_2 \ldots, A_{\frac{n-1}{2}}$$

hat man eine Substitutionsgruppe, *welche immer holoedrisch isomorph mit der Gruppe der D ist**). Diese Gruppe ist folgendermassen definirt:

$$\left\{\begin{array}{l} (A_\lambda)\ S = \varrho^{\lambda^2} A_\lambda; \qquad (A_\lambda)\ U_a = \left(\frac{a}{n}\right) A_{|a\lambda|}; \\ \qquad\qquad \left(\lambda = 0, 1, 2 \ldots \frac{n-1}{2}\right) \\ (A_0)\ T \cdot \left(\frac{\nu}{n}\right) \cdot i^{\left(\frac{n-1}{2}\right)^2} \cdot \sqrt{n} = A_0 + A_1 + \cdots + A_{\frac{n-1}{2}}; \\ (A_\alpha)\ T \cdot \left(\frac{\nu}{n}\right) \cdot i^{\left(\frac{n-1}{2}\right)^2} \cdot \sqrt{n} = 2A_0 + (\varrho^{-2\alpha} + \varrho^{2\alpha}) A_1 + (\varrho^{-4\alpha} + \varrho^{4\alpha}) A_2 + \cdots \\ \qquad + \left(\varrho^{-2\frac{n-1}{2}\alpha} + \varrho^{2\frac{n-1}{2}\alpha}\right) A_{\frac{n-1}{2}}; \quad \left(\alpha = 1, 2 \ldots \frac{n-1}{2}\right), \end{array}\right.$$

wo:

$$\varrho = e^{\frac{2\pi i}{n}\nu}\ **)$$

und $|a\lambda|$ in der Formel für U_a den absolut kleinsten Rest bedeutet, den $\pm a\lambda$ modulo n besitzt.

Vermöge des Klein'schen Fundamentalsatzes erhält man leicht für das Bildungsgesetz der A aus den D folgende Ausdrücke:

---

*) Diese A sind die sogenannten Jacobi'schen Theilgrössen. Vergl. Klein, Mathemat. Ann. Bd. XV, S. 276.

**) Man erkennt leicht, dass die Ausdrücke

$$\left(\frac{\nu}{n}\right) \cdot i^{\left(\frac{n-1}{2}\right)^2} \cdot \sqrt{n} \cdot A_0,$$

$$A_0 + \sum_{\alpha=1}^{\alpha=\frac{n-1}{2}} \varrho^{k\alpha^2} A_\alpha, \quad (k = 0, 1 . 2 \ldots n-1),$$

sich wie die D verhalten.

$$\begin{cases} A_0 = \left(\frac{\nu}{n}\right) \cdot i^{\left(\frac{n-1}{2}\right)^2} \cdot \sqrt{n} \cdot D_\infty + \sum_{k=0}^{n-1} D_k; \\ A_\alpha = 2 \sum_{k=0}^{n-1} \varrho^{-\alpha^2 k} D_k. \end{cases}$$

Durch diese Formeln ist die Frage nach der Bildung des A-Systems *vollständig* gelöst. Für $n = 5$ stimmen dieselben mit einem bekannten Resultate von Hrn. Brioschi überein (Atti dell' Istituto Lombardo, II, 1858).

§ 6.

In der wiederholt angeführten Abhandlung im XV. Bande dieser Annalen hat Prof. Klein erkannt, dass allgemein bei $\frac{n-1}{2}$ Variabeln

$$B_1, B_2, B_3 \ldots B_{\frac{n-1}{2}}$$

eine Substitutionsgruppe existirt, welche, *falls* $n \equiv 1$ (*mod.* 4) *mit der Gruppe* Γ *holoedrisch, falls* $n \equiv -1$ (*mod.* 4) *mit* Γ *hemiedrisch isomorph ist*, d. h. im letzteren Falle nur $\frac{n(n^2-1)}{2}$ Operationen enthält. Diese Gruppe ist, unserer gewöhnlichen Erzeugungsweise gemäss, folgendermassen definirt:

$$\begin{cases} (B_\alpha)\ S = \varrho^{\alpha^2} B_\alpha; \\ (B_\alpha)\ U_\alpha = \gamma \left(\frac{a}{n}\right) A_{\alpha a \nu}; \\ -\left(\frac{\nu}{n}\right) i^{\left(\frac{n-1}{2}\right)^2} \cdot \sqrt{n} \cdot (B_\alpha)\ T = (\varrho^{2\alpha} - \varrho^{-2\alpha}) B_1 + (\varrho^{4\alpha} - \varrho^{-4\alpha}) B_2 + \cdots \\ \qquad + \left(\varrho^{2\frac{n-1}{2}\alpha} - \varrho^{-2\frac{n-1}{2}\alpha}\right) B_{\frac{n-1}{2}}, \end{cases}$$

wo $\varrho = e^{\frac{2\pi i}{n}\nu}$, und γ, entweder $+1$ oder -1 bedeutet, jenachdem der Modulo n genommene kleinste Rest von αa positiv oder negativ ist.

Bei der Bildung dieser Variabeln B mittelst des Fundamentalsatzes gebrauchen wir zunächst eine willkürliche Function φ der Φ und irgend eine (v_β) der zu den B contragredienten Variabeln *). Wir bekommen so:

$$B_\alpha = \left(\frac{\alpha\beta}{n}\right) \sum_{k=0}^{n-1} \varrho^{-\beta^2 k} \left[(\varphi)\ S^k U_{\frac{\alpha}{\beta}} - \left(\frac{-1}{n}\right) (\dot{\varphi})\ S^k\ U_{-\frac{\alpha}{\beta}} \right]$$

$$- \left(\frac{\nu}{n}\right) \cdot \frac{i^{\left(\frac{n-1}{2}\right)^2}}{\sqrt{n}} \cdot \sum_{k=0}^{n-1} \sum_{l=1}^{n-1} \sum_{k=0}^{n-1} \left(\frac{l}{n}\right) \varrho^{-\beta^2 k - \alpha^2 k'} \cdot \left[\varrho^{-2\alpha\beta l} - \varrho^{2\alpha\beta l}\right] (\varphi)\ S^k U_l T S^{k'},$$

*) Siehe Annalen XV, l. c.

wo β die Zahlen $1, 2, 3 \ldots \frac{n-1}{2}$ bedeuten soll. Tragen wir nun in diese Ausdrücke für φ hinterher die Φ selbst ein, so erhält man nach einigen Reductionen mittelst der Gauss'schen Summen folgendes Resultat:

$$B_\alpha^{(\sigma)} = \left(\frac{\alpha}{n}\right) \sum_{k=0}^{n-1} \varrho^{-k\alpha} \left[\Phi_{\alpha\sigma, k\sigma} - \left(\frac{-1}{n}\right) \Phi_{-\alpha\sigma, -k\sigma} \right],$$

wo σ die Werthe $1, 2, 3 \ldots \frac{n-1}{2}$ annehmen kann.

Die allgemeinsten B sind dann:

$$B_\alpha = \sum_{\sigma=1}^{\sigma=\frac{n-1}{2}} \lambda_\sigma B_\alpha^{(\sigma)},$$

wo die λ bei den Substitutionen von Γ unveränderliche Functionen bezeichnen.

Diese lineare Zusammensetzung wird natürlich überflüssig, wenn man unter den Φ von vorneherein die allgemeinsten nach § 3 aufgebauten Φ verstehen will. Wenn die Φ die Theilwerthe einer ungeraden elliptischen Function sind, und $\left(\frac{-1}{n}\right)$ ist $= -1$, so verschwinden die so gebildeten B natürlich identisch; aber dies kann sofort vermieden werden, indem man die Φ durch irgend eine gerade Potenz derselben ersetzt*).

Leipzig, den 3. August 1884.

*) Die Vertauschungsgruppe der geraden Potenzen der Φ ist in diesem Falle holoedrisch isomorph mit der B-Gruppe.