72. Über die Invarianten der endlichen Gruppen halblinearer Transformationen.

Von Kenjiro SHODA.
Mathematical Institute, Osaka Imperial University.
(Comm. by T. TAKAGI, M.I.A., Oct. 12, 1938.)

In einer früheren Arbeit habe ich gemeinsam mit T. Nakayama die Darstellungen endlicher Gruppen durch halblineare Transformationen untersucht.[1] Daranschliessend werde ich in der vorliegenden Note den Invariantenbegriff für die halblinearen Transformationsgruppen einführen, der eine naturgemässe Verallgemeinerung des üblichen Invariantenbegriffes in der Theorie der linearen Transformationen bildet.

§ 1. Absolute Invariante.

Es sei K ein Körper von der Charakteristik Null; $S, T, \dots$ seine Automorphismen. Ist $\mathfrak{G}$ eine Gruppe, die aus den halblinearen Transformationen $x'_i=\sum_{j=1}^{n} a_{ij}x_j^S$ oder kurz $x'=Ax^S$ besteht, so bilden die darauftretenden Automorphismen $S, T, \dots$ eine Gruppe $\mathfrak{A}$, die einer Faktorgruppe $\mathfrak{G}/\mathfrak{H}$ isomorph ist. $\mathfrak{A}$ ist die galoissche Gruppe von K in bezug auf einen Unterkörper k.

Definition 1. Ein Polynom $F(x_1, x_2, \dots, x_n)$ oder kurz $F(x)$ heisst eine (absolute) Invariante von $\mathfrak{G}$, wenn $F(A^{-1}x^S)=F(x)^S$ für jede halblineare Transformation $x'=Ax^S$ aus $\mathfrak{G}$ ist.

Sind die S sämtlich identischer Automorphismus von K, so ist $\mathfrak{G}$ eine lineare Transformationsgruppe und $F(x)$ ist nichts anderes als Invariante im üblichen Sinne. Enthält $F(x)$ auf der anderen Seite keinen Variabel x, so ist also ein Element aus K dann und nur dann Invariante, wenn es in k enthalten ist. Im allgemeinen ist jede Invariante von $\mathfrak{G}$ sicher Invariante der linearen Transformationsgruppe $\mathfrak{H}$.

Die Gesamtheit der Invarianten von $\mathfrak{H}$ des Grades m bildet einen K-Modul. Sind $F_1(x), F_2(x), \dots, F_r(x)$ die Basiselemente, so werden sie bei den Transformationen aus $\mathfrak{G}$ so transformiert, dass man dadurch eine Darstellung von $\mathfrak{G}$ durch halblineare Transformationen erhält. Dies erkennt man leicht, wenn man $x_1, x_2, \dots, x_n$ als die Basiselemente des Darstellungsmoduls von $\mathfrak{G}$ betrachtet. Die Invariante von $\mathfrak{G}$ bzw. $\mathfrak{H}$ bildet dann die Basis eines identischen Darstellungsmoduls von $\mathfrak{G}$ bzw. $\mathfrak{H}$. Sind in der Tat $x_1, x_2, \dots, x_n$ die Basis des Darstellungsmoduls von $\mathfrak{G}$, so wird $F(x)$ durch einen Operator aus $\mathfrak{G}$ in $F^S(x')$ übergeführt, wobei $x'=Ax$ und $F^S(x)$ ein Polynom bedeutet, das man erhält, wenn man die Koeffizienten von $F(x)$ durch S transformiert. Ist die durch $F(x)$ vermittelte Darstellung eine identische, so muss $F(x)=F^S(x')$ sein.

---

1) T. Nakayama und K. Shoda, Über die Darstellung einer endlichen Gruppe durch halblineare Transformationen, Jap. Journal, **12** (1936), 109–122. Vgl. auch M. Osima, Über die Darstellung einer Gruppe durch halblineare Transformationen, Proc. Physico-Math. Soc. Japan, **20** (1938), 1–5.

Wenn man nun x durch x^S erstzt, so ergibt sich $F(x)^S = F(A^{-1}x^S)$. Also erhält man dadurch eine neue Fassung der Definition der Invariante. (Dann kann man die halblinearen Transformationen aus $\mathfrak{G}$ als Automorphismen des Polynombereiches $K[x_1, x_2, \cdots, x_n]$ auffassen.) Jede Invariante von $\mathfrak{H}$ wird ferner durch den Operator aus $\mathfrak{G}$ wieder in die Invariante von $\mathfrak{H}$ übergeführt da $\mathfrak{H}$ ein Normalteiler von $\mathfrak{G}$ ist.

Bei der eben konstruierten Darstellung entsprechen den Elementen aus $\mathfrak{H}$ die Einheitsmatrix, also ist die Darstellung in der Tat eine verschränkte Dastellung mit dem Faktorensystem Eins von $\mathfrak{A}$, also von $\mathfrak{G}/\mathfrak{H}$. Ist $\mathfrak{A}$ eine endliche Gruppe, so lässt sich die Darstellung auf identische Darstellungen reduziert, da das Faktorensystem aus Eins besteht. Die Basiselemente des identischen Darstellungsmoduls sind nach der Definition die Invarianten von $\mathfrak{G}$. Die Invariante von $\mathfrak{H}$ des Grades m lässt sich als lineare Verbindung solcher Invarianten von $\mathfrak{G}$ darstellen. Daher gilt, wenn $\mathfrak{A}$ eine endliche Gruppe ist:

Satz 1. *Man kann endlich viele Formen des Grades m so annehmen, dass jede Invariante von $\mathfrak{G}$ bzw. $\mathfrak{H}$ des Grades m lineare Verbindung der Formen mit Koeffizienten aus k bzw. K ist und umgekehrt.*

Der aus den sämtlichen Invarianten von $\mathfrak{H}$ bestehende Ring sei $K[F_1, F_2, \cdots, F_k]$, d. h. der Polynombereich der endlich vielen Invarianten F_i mit Koeffizienten aus K. Dies ist immer der Fall, wenn $\mathfrak{G}$ eine endliche Gruppe ist. Nach Satz 1 kann man die F_i so annehmen, dass sie zugleich Invarianten von $\mathfrak{G}$ sind. Bezeichnet man den aus den sämtlichen Invarianten von $\mathfrak{G}$ bestehenden Ring mit $\mathfrak{F}$, so ist $K[F_1, F_2, \cdots, F_k] \geq \mathfrak{F} \geq k[F_1, F_2, \cdots, F_k]$. Übergehend zum Quotientenkörper erhält man, wenn man den Quotientenkörker von $\mathfrak{F}$ mit $\mathfrak{F}^*$ bezeichnet, $K(F_1, F_2, \cdots, F_k) \geq \mathfrak{F}^* \geq k(F_1, F_2, \cdots, F_k)$. Der Durchschnitt von K und $\mathfrak{F}^*$ ist nach der Definition der Invariante gleich k. Nach der galoisschen Theorie ist also $\mathfrak{F}^* = k(F_1, F_2, \cdots, F_k)$ und folglich $\mathfrak{F} = k[F_1, F_2, \cdots, F_k]$. Damit erhält man, wenn $\mathfrak{G}$ etwa eine endliche Gruppe ist

Satz 2. *Man kann endlich viele Polynome $F_1, F_2, \cdots, F_k$ so annehmen, dass jede Invariante von $\mathfrak{G}$ bzw. $\mathfrak{H}$ Polynom von den F mit Koeffizienten aus k bzw. K ist, und umgekehrt. Daher ist der Invariantenbereich von $\mathfrak{G}$ endlich in bezug auf k.*

§ 2. Relative Invariante.

Definition 2. Die relative Invariante definieren wir durch $F(A^{-1}x^S) = c(A, S)\,F(x^S)$ mit $c(A, S)$ aus K.

Dann ist $F(x)$ natürlich eine relative Invariante von $\mathfrak{H}$, und die $c(A, S)$ bilden eine Darstellung von $\mathfrak{G}$ durch halblineare Transformationen ersten Grades.

Eine Darstellung von $\mathfrak{G}$ durch halblineare Transformationen reduziert sich dann und nur dann auf die Diagonalmatrizen, wenn dasselbe für die entsprechende Darstellung von $\mathfrak{H}$ gilt, und ferner, wenn die folgenden beiden Bedinungen erfüllt sind.[1]

Es sei eine lineare Darstellung $L_{\mathfrak{H}}$ von $\mathfrak{H}$ vorgegeben. Sie induziert eine irreduzible Darstellung von $\mathfrak{G}$ durch halblineare Transformationen

1) Vgl. hierzu die in der Anmerkung 1) zitierten Arbeiten.

und zwar induzieren zwei lineare Darstellungen dann und nur dann dieselbe Darstellung von $\mathfrak{G}$, wenn sie in $\mathfrak{G}$ konjugiert sind. Reduziert sich eine Darstellung von $\mathfrak{G}$ auf die Diagonalform, so müssen die durch die darauftretende lineare Darstellung von $\mathfrak{H}$ induzierten Darstellungen den Grad 1 haben. Daher erkennt man die Notwendigkeit der

Bedingung 1: Die betreffende lineare Darstellungen müssen mit ihren in $\mathfrak{G}$ konjugierten Darstellungen übereinstimmen.

Ist diese Bedingung erfüllt, so entsprechen den Elementen aus $\mathfrak{H}$ die Elemente aus K, falls die Darstellung von $\mathfrak{G}$ irreduzibel ist. Daher kann man die Darstellung als eine verschränkte Darstellung von $\mathfrak{A}$ auffassen, deren Faktorensystem aus Einheitswurzeln besteht. Damit der Grad dieser Darstellung gleich 1 sei, ist nach der Algebrentheorie notwendig und hinreichend, dass das Faktorensystem zu Eins assoziiert ist:

Bedingung 2: Das oben erhaltene Faktorensystem soll zu Eins assoziiert sein.

Sind diese beiden Bedingungen erfüllt für eine lineare Darstellung $L_{\mathfrak{H}}$ von $\mathfrak{H}$, so kann man wie bei § 1 vorgehen und schliessen:

Satz 3. *Man kann endlich viele Formen des Grades m so annehmen, dass jede zur linearen Darstellung $L_{\mathfrak{H}}$ gehörige Invariante von $\mathfrak{H}$ bzw. jede zur durch $L_{\mathfrak{H}}$ induzierten Darstellung gehörige Invariante von $\mathfrak{G}$ lineare Verbindung der Formen mit Koeffizienten aus K bzw. k ist und umgekehrt.*

Nun werden wir die Bedingungen 1 und 2 genauer untersuchen. Die lineare Darstellung $L_{\mathfrak{H}}$ ist einer zyklischen Faktorgruppe $\mathfrak{H}/\mathfrak{L}$ isomorph. Die Bedingung 1 besagt, dass $\mathfrak{H}/\mathfrak{L}$ bei den Transformationen durch die Elemente aus $\mathfrak{G}$ elementweise invariant bleibt. Bezeichnet man die Kommutatorgruppe von $\mathfrak{H}$ mit $\mathfrak{K}$, so bewirkt ein Element aus $\mathfrak{G}$ einen Automorphismus von $\mathfrak{H}/\mathfrak{K}$. Damit ist das Problem auf das folgende Problem über die Automorphismen einer endlichen abelschen Gruppe reduziert. Man hat zu bestimmen die sämtlichen zyklischen Faktorgruppen $\mathfrak{A}/\mathfrak{B}$ einer abelschen Gruppe $\mathfrak{A}$, die bei gewissen Automorphismen von $\mathfrak{A}$ elementweise invariant bleiben.

Bleiben aber zwei Faktorgruppen $\mathfrak{A}/\mathfrak{B}_1$, $\mathfrak{A}/\mathfrak{B}_2$ bei den vorgegebenen Automorphismen elementweise invariant, so gilt dasselbe auch für die Faktorgruppe $\mathfrak{A}/\mathfrak{D}$ nach dem Durchschnitt $\mathfrak{D}=[\mathfrak{B}_1, \mathfrak{B}_2]$. Denn ein Element a aus $\mathfrak{A}$ wird durch den Automorphismus in ab_1, ab_2 übergeführt, wobei b_1 bzw. b_2 Element aus $\mathfrak{B}_1$ bzw. $\mathfrak{B}_2$ bedeutet. Daher ist $b_1=b_2$ in $\mathfrak{D}$ enthalten und $\mathfrak{A}/\mathfrak{D}$ bleiben bei dem Automorphismus elementweise invariant.

Bezeichnet man das Invariantensystem von $\mathfrak{A}$ mit $a_1, a_2, \cdots, a_m$, wo a_i durch a_{i+1} teilbar ist, so wird eine Faktorgruppe $\mathfrak{A}/\mathfrak{B}$ durch eine Matrix B des Grades m definiert.[1] Sind nämlich $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_m$ die Basis der additiv geschriebenen abelschen Gruppe $\mathfrak{A}$, so gibt es eine Matrix B derart, dass $\mathfrak{B}$ durch die Koeffizienten der einzeiligen Matrix $(\varepsilon)B=(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_m)B$ erzeugt wird. Dabei kann man B als ein Linksteiler der Diagonalmatrix A mit Koeffizienten $a_1, a_2, \cdots, a_m$ annehmen. Dann

1) Vgl. etwa K. Shoda, Über die Automorphismen einer endlichen Abelschen Gruppe, Math. Ann. **100** (1928), 674–686.

stimmen die Invarianten von $\mathfrak{B}$ mit den Elementarteiler der Matrix B überein. Stellt man einen Automorphismus von A auch durch eine Matrix P dar, so besagt die Bedingung 1, dass $(\varepsilon)P-(\varepsilon)=(\varepsilon)BX$ mit ganzzahliger Matrix X ist, d. h. dass B ein Linksteiler der Matrizen $P-E$ und A ist. Die Existenz der minimalen Untergruppe $\mathfrak{B}$ besagt schon, dass man B als den grössten gemeinsamen Linksteiler der sämtlichen Matrizen $P-E$ und A annehmen kann. Diese Matrix ist bis auf unimodulären Rechtsteiler eindeutig bestimmt.

Existiert insbesondere eine Matrix P derart, dass $P-E$ auch einen eigentlichen Automorphismus bedeutet, so kann man $B=E$ annehmen und folglich $\mathfrak{B}=\mathfrak{A}$. In der Invariantentheorie gilt also: Gibt es ein Element p aus $\mathfrak{G}$ derart, dass $a \rightarrow pap^{-1}a^{-1}$ mit a aus $\mathfrak{H}/\mathfrak{K}$ einen eigentlichen Automorphismus bedeutet, so ist jede relative Invariante von $\mathfrak{G}$ eine absolute. Dies ist immer der Fall, wenn die Ordnung von $\mathfrak{H}/\mathfrak{K}$ ungerade ist und, wenn es ein Element p aus $\mathfrak{G}$ mit $pap^{-1}=a^2$ gibt.

Wir betrachten nun die Bedingung 2. Nach der Bedingung 1 nehmen wir jetzt an, dass ein minimaler Normalteiler $\mathfrak{L}$ von $\mathfrak{G}$ vorgegeben ist, derart, dass $\mathfrak{H}/\mathfrak{L}$ im Zentrum von $\mathfrak{G}/\mathfrak{L}$ enthalten ist. Bildet man eine irreduzible Darstellung von $\mathfrak{G}/\mathfrak{L}$ durch halblineare Transformationen, so erkennt man, dass sie in der Tat eine verschrankte Darstellung von $\mathfrak{G}/\mathfrak{H}$ ist. Das Faktorensystem erhält man durch Charakterbildung von $\mathfrak{H}/\mathfrak{L}$. Die Bedingung 2 verlangt, dass das Faktorensystem zu 1 assoziiert sein soll. Dies ist gerade das Problem, das R. Brauer und ich früher untersucht haben.[1] Man kann das Problem auf gewisses Problem in der Gruppentheorie sowie auf gewisses Einbettungsproblem in der Körpertheorie reduzieren.

§ 3. Beziehung mit der Körpertheorie.

Wir beweisen nun

Satz 4. *Ist $k(F_1, F_2, \cdots, F_k)$ der Invariantenkörper der endlichen halblinearen Transformationsgruppe $\mathfrak{G}$, so ist $K(x_1, x_2, \cdots, x_n)$ ein galoisscher Erweiterungskörper mit der zu $\mathfrak{G}$ isomorphen galoisschen Gruppe.*

Ersetzt man nämlich $f(x)$ aus $K(x)=K(x_1, x, \cdots, x_n)$ durch $f(A^{-1}x)$, so erhält man einen Automorphismus $\alpha(A)$ von $K(x)$. Ein Automorphismus η_S von $K(x)$ bzw. $K(x^S)$ wird auch durch einen Automorphismus S von K induziert. Einer halblinearen Transformation $x'=Ax^S$ sei ein Automorphismus $\alpha(A)\eta_S$ zugeordnet. Dann entspricht dem Produkt zweier halblinearer Transformationen das Produkt der entsprechenden Automorphismen. Man erkennt auch leicht, dass diese Zuordnung eine eineindeutige ist. Daher ist die Gruppe $\mathfrak{G}$ der halblinearen Transformationen zur Gruppe solcher Automorphismen isomorph.

Die Invariante $F(x)$ genügt nach § 1 der Gleichung $F^S(Ax)=F(x)$. Also ist F durch $\alpha(A)\eta_S$ invariant. Daher ist unsere Gruppe der Automorphismen eine Gruppe der Automorphismen von $K(x)$ in bezug auf

1) R. Brauer, Über die Konstruktion der Schiefkörper, die von endlichem Rang in bezug auf ein gegebenes Zentrum sind, Journal für Math. **168** (1932), 44-64.

K. Shoda, Über die endlichen Gruppen der Algebrenklassen mit einem Zerfällungskörper, Jap. Journal, **11** (1934), 21-30.

$k(F)=k(F_1, F_2, \ldots, F_k)$. Der Grad $(K:k)$ ist aber gleich der Ordnung von $\mathfrak{G}/\mathfrak{H}$ und der Grad $\big(K(x):k(F)\big)$ gleich der Ordnung von $\mathfrak{G}$. Daher ist $K(x)$ galoissch über $k(F)$ und die galoissche Gruppe ist zu $\mathfrak{G}$ isomorph. Damit ist der Satz bewiesen.

Als eine unmittelbare Folgerung erhält man hieraus

Satz 5. *Eine endliche Gruppe halblinearer Transformationen wird durch den zugrundliegenden Körper K und die Invarianten vollständig charakterisiert.*