Der Endlichkeitssatz der Invarianten endlicher Gruppen.

Von

Emmy Noether in Erlangen.

Im folgenden soll ein ganz elementarer — nur auf der Theorie der symmetrischen Funktionen beruhender — Endlichkeitsbeweis der Invarianten *endlicher* Gruppen gebracht werden, der zugleich eine *wirkliche Angabe des vollen Systems* liefert; während der gewöhnliche, auf das Hilbertsche Theorem von der Modulbasis (Ann. 36) sich stützende Beweis nur Existenzbeweis ist.*)

Die endliche Gruppe $\mathfrak{H}$ bestehe aus den h linearen Transformationen (von nichtverschwindender Determinante) $A_1 \cdots A_h$, wobei durch A_k die lineare Transformation

$$x_1^{(k)} = \sum_{\nu=1}^{n} a_{1\nu}^{(k)} x_\nu, \cdots, x_n^{(k)} = \sum_{\nu=1}^{n} a_{n\nu}^{(k)} x_\nu$$

oder abkürzend: $(x^{(k)}) = A_k(x)$ dargestellt sei. Die Gruppe $\mathfrak{H}$ führt also die Reihe (x) mit den Elementen $x_1 \cdots x_n$ über in die Reihen $(x^{(k)})$ mit den Elementen $x_1^{(k)} \cdots x_n^{(k)}$. Da unter $A_1 \cdots A_h$ die Identität enthalten sein muß, ist auch unter den Reihen $(x^{(k)})$ die Reihe (x) enthalten. — Unter einer ganzen rationalen (absoluten) Invariante der Gruppe sei eine solche ganze rationale Funktion von $x_1 \cdots x_n$ verstanden, die bei Anwendung von $A_1 \cdots A_h$ identisch ungeändert bleibt; für eine solche Invariante $f(x)$ gilt also:

$$(1) \qquad f(x) = f(x^{(1)}) = \cdots = f(x^{(k)}) = \frac{1}{h} \cdot \sum_{k=1}^{h} f(x^{(k)}).$$

1. Formel (1) drückt aus, daß $f(x)$ eine ganze rationale, *symmetrische* Funktion der Größenreihen $(x^{(1)}) \cdots (x^{(h)})$ ist — und zwar handelt es sich, da jeder Summand $f(x^{(k)})$ nur die *eine* Reihe $(x^{(k)})$ enthält, um den einfachsten, gewöhnlich als *einförmigen* bezeichneten Fall. Nach dem be-

*) Vgl. etwa Weber, Lehrbuch der Algebra (2. Aufl.) 2. Band, § 57.

kannten Satz über die symmetrischen Funktionen von Größen*reihen**) ist also $f(x)$ ganz und rational durch die symmetrischen Elementarfunktionen dieser Reihen darstellbar, d. h. durch die Koeffizienten $G_{\alpha\alpha_1\cdots\alpha_n}(x)$ der „Galoisschen Resolvente“:

$$\Phi(z,u)=\prod_{k=1}^{h}(z+u_1x_1^{(k)}+\cdots+u_nx_n^{(k)})$$
$$=z^h+\sum G_{\alpha\alpha_1\cdots\alpha_n}(x)\,z^{\alpha}u_1^{\alpha_1}\cdots u_n^{\alpha_n}\qquad\begin{pmatrix}(\alpha+\alpha_1+\cdots+\alpha_n=h)\\ \alpha\neq h\end{pmatrix}$$

wo die $G_{\alpha\alpha_1\cdots\alpha_n}(x)$ Invarianten vom Grade $\alpha_1+\cdots+\alpha_n$ in den x sind. Somit ist bewiesen:

Die Koeffizienten $G_{\alpha\alpha_1\cdots\alpha_n}(x)$ der Galoisschen Resolvente bilden ein volles Invariantensystem der Gruppe derart, daß jede Invariante sich ganz und rational durch diese endlich vielen Invarianten darstellen läßt.

2. Man kann auch, von (1) ausgehend, die folgende noch elementarere Betrachtung anstellen,**) die zugleich zu einem zweiten vollen System führt. Sei gesetzt

$$f(x)=a+bx_1^{\mu_1}\cdots x_n^{\mu_n}+\cdots+cx_1^{\nu_1}\cdots x_n^{\nu_n},$$

wo $a, b, \cdots, c$ Konstanten bedeuten, so hat man nach (1):

$$h\cdot f(x)=h\cdot a+b\cdot\sum_{k=1}^{h}x_1^{(k)^{\mu_1}}\cdots x_n^{(k)^{\mu_n}}+\cdots+c\cdot\sum_{k=1}^{h}x_1^{(k)^{\nu_1}}\cdots x_n^{(k)^{\nu_n}}$$
$$=h\cdot a+b\cdot J_{\mu_1\cdots\mu_n}+\cdots+c\cdot J_{\nu_1\cdots\nu_n}.$$

Jede Invariante läßt sich also ganz und linear aus den speziellen:

$$J_{\mu_1\cdots\mu_n}=\sum_{k=1}^{h}x_1^{(k)^{\mu_1}}\cdots x_n^{(k)^{\mu_n}}$$

zusammensetzen, und es genügt daher der Nachweis für diese speziellen. $J_{\mu_1\cdots\mu_n}$ bildet aber, abgesehen von einem Zahlenfaktor, den Koeffizient von $u_1^{\mu_1}\cdots u_n^{\mu_n}$ in dem Ausdruck

$$S_\mu=\sum_{k=1}^{h}(u_1x_1^{(k)}+\cdots+u_nx_n^{(k)})^{\mu},$$

wo $\mu=\mu_1+\cdots+\mu_n$ gesetzt ist, und der die μ^{te} Potenzsumme der h Linearformen

$$\xi_1=u_1x_1^{(1)}+\cdots+u_nx_n^{(1)},\ \cdots,\ \xi_h=u_1x_1^{(h)}+\cdots+u_nx_n^{(h)}$$

---

*) Vgl. die Anmerkung zu 2.

**) Es kommt dies auf einen Beweis des Satzes über die symmetrischen Funktionen von Größenreihen im oben erwähnten *einförmigen* Fall hinaus.

darstellt. Nun sind bekanntlich die unendlich vielen Potenzsummen S_μ ganze rationale Verbindungen von

$$S_1, S_2, \cdots, S_h,$$

deren Koeffizienten durch die Invarianten

$$J_{\mu_1 \cdots \mu_n} \qquad (\mu_1 + \cdots + \mu_n \leqq h)$$

gegeben sind; somit ist ein zweites volles System gewonnen:

Ein volles Invariantensystem der Gruppe ist gegeben durch alle Invarianten $J_{\mu_1 \cdots \mu_n}$, wo $\mu_1 + \cdots + \mu_n \leqq h$ und h die Ordnung der Gruppe bedeutet.

Der Zusammenhang mit 1. wird hergestellt durch die Bemerkung, daß die Potenzsummen $S_1 \cdots S_h$ sich durch die elementaren symmetrischen Funktionen von $\xi_1 \cdots \xi_h$ ersetzen lassen, was auf das dort gegebene volle System der $G_{\alpha\alpha_1 \cdots \alpha_n}(x)$ führt. Beide Resultate zeigen, daß sich *alle Invarianten ganz und rational durch diejenigen ausdrücken lassen, deren Grad in den x die Ordnung h der Gruppe nicht übersteigt.*

3. Aus dem eben Bewiesenen lassen sich Folgerungen für rationale Darstellung ziehen. Jede *rationale* absolute Invariante läßt sich — wie durch Erweiterung von Zähler und Nenner mit den in bezug auf die Gruppe Konjugierten des Nenners unmittelbar einzusehen — darstellen als Quotient von zwei, nicht notwendig teilerfremden, ganzen rationalen absoluten Invarianten. Daraus folgt, daß *jede rationale absolute Invariante sich rational durch die Koeffizienten $G_{\alpha\alpha_1 \cdots \alpha_n}(x)$ der Galoisschen Resolvente $\Phi(z, u)$ ausdrücken läßt.* Dieser Satz läßt sich auch ohne Durchgang durch den Endlichkeitssatz auf verschiedene Art leicht beweisen; er findet sich schon formuliert in Weber II, § 58.*)

---

*) Der dort gegebene Beweis ist allerdings nicht stichhaltig; es ist nämlich nur gezeigt, daß die Funktion $\Psi(t)$ in Formel (7) Invarianten zu Koeffizienten hat, nicht aber daß diese Invarianten rational durch die Koeffizienten von $\Phi(t)$ ausdrückbar sind. Diese Lücke wird vermieden, wenn man zur Darstellung der $x_i^{(k)}$ durch ξ_k statt der Lagrangeschen Interpolationsformel ein bekanntes Differentiationsverfahren anwendet. Es ist dies die durch Differentiation der Identität $\Phi(-\xi_k, u) = 0$ nach allen u gewonnene Relation:

$$\left[\frac{\partial \Phi}{\partial u_i} - x_i^{(k)} \cdot \frac{\partial \Phi}{\partial z}\right]_{z=-\xi_k} = 0.$$

Danach hat an Stelle von Formel (7) und (8) bei Weber für jede rationale Funktion $\omega(x)$ die folgende Formel zu treten:

$$\omega(x_1^{(k)} \cdots x_n^{(k)}) = \omega\left(\frac{\dfrac{\partial \Phi}{\partial u_1}}{\dfrac{\partial \Phi}{\partial z}} \cdots \frac{\dfrac{\partial \Phi}{\partial u_n}}{\dfrac{\partial \Phi}{\partial z}}\right)_{z=-\xi_k},$$

4. Schließlich sei erwähnt, daß die hier abgeleiteten Resultate implizit enthalten sind in meiner Arbeit „Körper und Systeme rationaler Funktionen“*); und zwar das in 1. gegebene volle System in Satz VI und VII, ein von diesem Endlichkeitssatz unabhängiger Beweis der rationalen Darstellung in Satz III.**) Beweisgang und Resultat vereinfachen sich aber in dem hier vorliegenden speziellen Fall erheblich gegenüber der allgemeinen Theorie. Darauf, die allgemeinen Untersuchungen auf die Invarianten endlicher Gruppen anzuwenden, kam ich durch Gespräche mit Herrn E. Fischer, von dem auch dem Inhalt nach der unter 2. gegebene Beweis — im allgemeinen Fall ist das dort auftretende volle System nicht rational definierbar — und die Anmerkung zu 3. herrührt.

Erlangen, Mai 1915.

---

die nur noch Koeffizienten von $\Phi(z, w)$ enthält, und deren Summation über alle k für Invarianten $\omega(x)$ die gewünschte Darstellung gibt.

*) Math. Ann. 76, S. 161 (1915).

**) Für *relative* Invarianten ist in Satz VIII und IX ein Endlichkeitsbeweis enthalten, der ebenfalls auf anderer Grundlage beruht als der gewöhnliche, aber auch nur Existenzbeweis ist; es rührt dies daher, daß die relativen Invarianten keinen Körper bilden.