

29. Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p .

Nachr. v. d. Ges. d. Wiss. zu Göttingen 1926, S. 28–35

Vorgelegt von R. Courant in der Sitzung vom 30. Juli 1926.

Ich zeige im folgenden, daß der bekannte Endlichkeitssatz der Invarianten endlicher Gruppen linearer Substitutionen¹⁾ erhalten bleibt, wenn als Koeffizientenbereich statt eines gewöhnlichen Zahlkörpers ein beliebiger Körper — also insbesondere der Charakteristik p ²⁾ zugrunde gelegt wird. Dabei versagen aber die bekannten Endlichkeitsbeweise, sobald die Ordnung der Gruppe durch p teilbar wird; es müssen tieferliegende arithmetische Tatsachen herangezogen werden, nämlich das folgende bisher nur für Charakteristik Null bekannte

Endlichkeitskriterium³⁾: Ein Integritätsbereich $\mathfrak{S}$ aus Polynomen — allgemeiner aus rationalen Funktionen — mit Koeffizienten aus einem Körper, ist dann und nur dann ein endlicher, wenn in $\mathfrak{S}$ ein endlicher Unterring $\mathfrak{R}$ enthalten ist derart, daß $\mathfrak{S}$ algebraisch ganz von $\mathfrak{R}$ abhängt. Jede Integritätsbasis von $\mathfrak{R}$ wird dann durch eine Modulbasis von $\mathfrak{S}$ in bezug auf einen gewissen Unterring von $\mathfrak{R}$ zu einer Integritätsbasis von $\mathfrak{S}$ ergänzt.

Dieses Kriterium — das an sich von selbständigem Interesse ist — beruht auf der Existenz der Rationalbasis und auf der Tat-

1) Für einen elementaren Endlichkeitsbeweis vergl. E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen. Math. Ann., 77 (1916), S. 89–92.

2) Für die Begriffe der Körpertheorie vergl. E. Steinitz, Algebraische Theorie der Körper. J. f. M., 137 (1910), S. 167–309. Charakteristik in § 4, Wurzelkörper in § 12, Quotientenkörper in § 3.

3) Vergl. E. Noether, Algebraische und Differentialinvarianten. Jahresber. d. d. Math.-Ver., 32 (1923), S. 177–184, Nr. 3, Satz 4 und die dort angegebene Literatur. Im letzten Satz des Kriteriums steht dort fälschlich „Modulbasis in bezug auf $\mathfrak{R}$ “ (Fundamentalsystem der ganzen Größen) statt „in bezug auf einen gewissen Unterring von $\mathfrak{R}$ “.

sache, daß der Teilerkettensatz erhalten bleibt beim Übergang zu den ganzen Größen einer endlichen Erweiterung. Dieser zweite Satz ist in der vorangehenden Note von Artin und v. d. Waerden für beliebige Charakteristik bewiesen nur unter Zugrundelegung einer gewissen, im Fall der endlichen Gruppen erfüllten Endlichkeitsvoraussetzung für den ursprünglichen Bereich (der Wurzelring stellt eine endliche Erweiterung dar). Für die Existenz der Rationalbasis gebe ich einen für beliebige Körper als Koeffizientenbereich gültigen Beweis; damit kann ich das Endlichkeitskriterium unter der obigen Einschränkung beweisen

Daß für Invarianten endlicher Gruppen das Endlichkeitskriterium erfüllt ist, beruht auf dem Prinzip der symmetrischen Funktionen. Während aber bei Charakteristik Null die Koeffizienten der Galois'schen Resolvente schon die Integritätsbasis liefern, erzeugen sie im allgemeinen Fall nur den im Endlichkeitskriterium verlangten endlichen Unterring. Aus der Existenz dieses endlichen Unterrings folgt nach denselben Schlüssen die Endlichkeit der „Relativ“-Invarianten und der „Modular“-Invarianten.

Unter die hier betrachteten Invarianten fallen als Spezialfälle die von Dickson und seiner Schule¹⁾ behandelten „projektiven Invarianten mod p “. Hier war zwar für Modular-Invarianten, nicht aber für allgemeine „formale“ Invarianten, der Endlichkeitssatz bekannt.

§ 1. Das Endlichkeitskriterium.

1. Satz von der Existenz der Rationalbasis. Erste Fassung: Jedes System S rationaler Funktionen von n Unbestimmten, mit Koeffizienten aus einem Körper P , besitzt eine endliche Rationalbasis; d. h. es gibt endlich viele Funktionen des Systems derart, daß jede Funktion des Systems sich rational, mit Koeffizienten aus P , durch diese endlich vielen ausdrücken läßt.

Zweite Fassung: Sei $\mathfrak{K}$ Zwischenkörper von P und $P(x_1, \dots, x_n)$ — wo $x_1, \dots, x_n$ Unbestimmte bedeuten — von einem Transzendenzgrad $t \leq n$; sei $y_1, \dots, y_t$ ein irreduzibles System²⁾ aus $\mathfrak{K}$. Dann wird $\mathfrak{K}$ endliche algebraische Erweiterung von $P(y_1, \dots, y_t)$.

1) Vergl. Dickson, On Invariants and the theory of Numbers. The Madison Colloquium 1913. Neuere Literatur in den seitdem erschienenen Bänden der Transactions of the American Mathematical Society.

2) Ein System heißt nach Steinitz irreduzibel, wenn es aus algebraisch unabhängigen Funktionen besteht. Ein System heißt vom Transzendenzgrad t , wenn es mindestens ein irreduzibles System aus t Elementen, aber keines aus mehr Elementen enthält. Für die im folgenden benutzten einfachen Sätze über irreduzible Systeme vergl. Steinitz, § 22.

Die beiden Fassungen sind tatsächlich äquivalent. Es genügt nämlich die Existenz der Rationalbasis für alle Zwischenkörper zu beweisen; denn der aus einem System S abgeleitete Körper wird ein solcher Zwischenkörper $\mathfrak{K}$, dessen Rationalbasis unmittelbar eine Rationalbasis von S ergibt, da jedes Element aus $\mathfrak{K}$ rationale Verbindung von endlich vielen Funktionen aus S wird. Aus der zweiten Fassung folgt aber, daß ein beliebiges irreduzibles System $y_1, \dots, y_t$ aus $\mathfrak{K}$, vermehrt um die endlich vielen Funktionen, die $\mathfrak{K}$ als endliche Erweiterung von $P(y_1, \dots, y_t)$ charakterisieren, eine solche Rationalbasis ergibt. Ist umgekehrt nach der ersten Fassung eine Rationalbasis von $\mathfrak{K}$ gegeben, so muß nach Definition des Transzendenzgrades jedes Basiselement algebraisch abhängig von $P(y_1, \dots, y_t)$ sein; also wird dadurch $\mathfrak{K}$ als endliche algebraische Erweiterung von $P(y_1, \dots, y_t)$ charakterisiert.

Der Satz soll in der zweiten Fassung bewiesen werden. Sei vorerst $\mathfrak{K}$ vom selben Transzendenzgrad n wie $P(x_1, \dots, x_n)$; sei $y_1, \dots, y_n$ ein irreduzibles System aus $\mathfrak{K}$ und folglich aus $P(x_1, \dots, x_n)$. Wegen des Transzendenzgrades n von $y_1, \dots, y_n$ wird jedes x_i algebraisch über $P(y_1, \dots, y_n)$; also wird $P(x_1, \dots, x_n)$ und damit $\mathfrak{K}$ als Zwischenkörper endliche algebraische Erweiterung von $P(y_1, \dots, y_n)$.

Sei jetzt $t < n$; sei die Numerierung der x so gewählt, daß $y_1, \dots, y_t, x_{t+1}, \dots, x_n$ ein irreduzibles System aus $P(x_1, \dots, x_n)$ bilden. Es wird also $x_{t+1}, \dots, x_n$ irreduzibel inbezug auf $P(y_1, \dots, y_t)$ und damit nach dem transitiven Gesetz der algebraischen Abhängigkeit auch irreduzibel inbezug auf $\mathfrak{K}$ und auf jeden Zwischenkörper $\mathfrak{M}$ von $P(y_1, \dots, y_t)$ und $\mathfrak{K}$. Das heißt aber, daß $\bar{\mathfrak{K}} = \bar{\mathfrak{K}}(x_{t+1}, \dots, x_n)$ bzw. $\bar{\mathfrak{M}} = \bar{\mathfrak{M}}(x_{t+1}, \dots, x_n)$ rein transzendente Erweiterung von $\mathfrak{K}$ bzw. $\mathfrak{M}$ wird; daß also jedes nicht zu $\mathfrak{K}$ gehörige Element aus $\bar{\mathfrak{K}}$ transzendent inbezug auf $\mathfrak{K}$ wird, ebenso jedes nicht zu $\mathfrak{M}$ gehörige Element aus $\bar{\mathfrak{M}}$ transzendent inbezug auf $\mathfrak{M}$. Ebenso sei $\bar{P}$ gleich der rein transzendenten Erweiterung $P(x_{t+1}, \dots, x_n)$ gesetzt; dann wird $y_1, \dots, y_t$ irreduzibel inbezug auf $\bar{P}$.

Der Beweis wird sich jetzt auf den oben erledigten zurückführen lassen dadurch, daß $\bar{P}$ als Koeffizientenbereich zugrunde gelegt wird. Aus $P < \mathfrak{K} < P(x_1, \dots, x_t; x_{t+1}, \dots, x_n)$ ¹⁾ folgt nämlich: $\bar{P} < \bar{\mathfrak{K}} < \bar{P}(x_1, \dots, x_t)$, wobei $\bar{\mathfrak{K}}$ vom gleichen Transzendenzgrad t inbezug auf $\bar{P}$ wird wie $\bar{P}(x_1, \dots, x_t)$. Somit besitzt $\bar{\mathfrak{K}}$ inbezug auf $\bar{P}$ als Koeffizientenbereich eine endliche Rationalbasis, etwa $y_1, \dots, y_t; z_1, \dots, z_s$. Dabei können die z aus $\mathfrak{K}$ gewählt werden, da $\mathfrak{K}$ Ver-

1) $P < \mathfrak{K}$ heißt: P ist in $\mathfrak{K}$ enthalten, also Unterkörper von $\mathfrak{K}$.

einigungskörper von $\mathfrak{K}$ und $\bar{\mathfrak{P}}$ ist. Es ist zu zeigen, daß $\mathfrak{K}$ gleich $\mathfrak{M} = \mathfrak{P}(y_1, \dots, y_t; z_1, \dots, z_s)$ wird. Es wird $\mathfrak{M}$ Zwischenkörper von $\mathfrak{P}(y_1, \dots, y_t)$ und $\mathfrak{K}$; also ist jedes Element von $\mathfrak{K}$ algebraisch in bezug auf $\mathfrak{M}$. Andererseits wird $\mathfrak{M}$ gleich $\bar{\mathfrak{K}}$ und somit ist $\mathfrak{K}$ in $\bar{\mathfrak{M}}$ enthalten. Es wird also $\mathfrak{K}$ Zwischenkörper von $\mathfrak{M}$ und $\bar{\mathfrak{M}}$, und da jedes nicht zu $\mathfrak{M}$ gehörige Element aus $\bar{\mathfrak{M}}$ transzendent in bezug auf $\mathfrak{M}$ ist, so wird notwendig $\mathfrak{K}$ mit $\mathfrak{M}$ identisch.

Folgerung: Ist $\mathfrak{P} < \mathfrak{K} < \mathfrak{L} < \mathfrak{P}(x_1, \dots, x_n)$, und ist $\mathfrak{L}$ algebraisch in bezug auf $\mathfrak{K}$, so ist $\mathfrak{L}$ endliche algebraische Erweiterung von $\mathfrak{K}$. Denn jedes Element einer Rationalbasis von $\mathfrak{L}$ ist dann algebraisch in bezug auf $\mathfrak{K}$; somit wird $\mathfrak{L}$ als endliche Erweiterung von $\mathfrak{K}$ charakterisiert.

2. Beweis des Endlichkeitskriteriums. Die Bedingung ist offenbar notwendig; denn wenn $\mathfrak{F}$ endlicher Integritätsbereich ist, so läßt sich $\mathfrak{F}$ selbst als der im Kriterium auftretende endliche Unterring $\mathfrak{K}$ auffassen.

Die Bedingung ist hinreichend unter der Voraussetzung, daß der Wurzelkörper $\mathfrak{P}^{1/p}$ endliche Erweiterung des Koeffizientenkörpers¹⁾, sobald dieser von Charakteristik p ; für Charakteristik Null ist keine einschränkende Voraussetzung nötig. Zum Nachweis ist zu zeigen, daß $\mathfrak{F}$ eine endliche Modulbasis in bezug auf einen Unterring von $\mathfrak{K}$ besitzt.

Es bedeute $\mathfrak{K}$ den Quotientenkörper¹⁾ von $\mathfrak{K}$ und $\mathfrak{L}$ den Quotientenkörper von $\mathfrak{F}$. Diese Quotientenkörper existieren, da es sich um Ringe ohne Nullteiler handelt; und es wird $\mathfrak{P} < \mathfrak{K} < \mathfrak{L} < \mathfrak{P}(x_1, \dots, x_n)$. Also wird $\mathfrak{L}$ nach der Folgerung unter 1. endlicher algebraischer Erweiterungskörper von $\mathfrak{K}$; es ist weiter nach Voraussetzung jedes Element aus $\mathfrak{F}$ ganz in bezug auf $\mathfrak{K}$, und es wird somit $\mathfrak{F}$ Unterring des aus allen $\mathfrak{K}$ -ganzen Elementen aus $\mathfrak{L}$ bestehenden Ringes $\mathfrak{G}$. Da aber nichts über die ganze Abgeschlossenheit von $\mathfrak{K}$ in $\mathfrak{K}$ vorausgesetzt ist, kann die Tatsache, daß bei endlicher Erweiterung der Teilerkettensatz erhalten bleibt, nicht direkt herangezogen werden. Es muß vielmehr erst zu einem gleichfalls endlichen Unterring $\mathfrak{T}$ von $\mathfrak{K}$ übergegangen werden, für den diese ganze Abgeschlossenheit erfüllt ist.

Es sei vorerst vorausgesetzt, daß der Koeffizientenbereich $\mathfrak{P}$ unendlich viele Elemente enthält. Dann läßt sich aus $\mathfrak{K}$ ein irreduzibles System $g_1(x), \dots, g_t(x)$ auswählen derart, daß $\mathfrak{K}$ und damit $\mathfrak{F}$ algebraisch ganz von $\mathfrak{T} = \mathfrak{P}[g_1(x), \dots, g_t(x)]$ abhängt. Bedeutet nämlich $f_1(x), \dots, f_k(x)$ die nach Voraussetzung existierende Inte-

1) Siehe S. 28, Fußnote 2.

Integritätsbasis von $\mathfrak{R}$, und bildet diese kein irreduzibles System, so sei — nach etwaiger Umnummerierung der Indizes — $F(f_k; f_1, \dots, f_{k-1}) = 0$ eine Relation, der f_k genügt. Ersetzt man $f_1, \dots, f_{k-1}$ durch

$$f_1 + t_1 f_k, \dots, f_{k-1} + t_{k-1} f_k;$$

so hängt f_k und damit auch $f_1, \dots, f_{k-1}$ algebraisch ganz von diesen neuen Funktionen ab, wenn die t_i als Unbestimmte gewählt werden; da P unendlich viele Elemente besitzt, lassen die t_i sich so zu Elementen aus P spezialisieren, daß diese ganze Abhängigkeit erhalten bleibt. Nach endlich vielen Schritten gelangt man also unter Beachtung des transitiven Gesetzes der ganzen Abhängigkeit zu dem gesuchten Ring $\mathfrak{T} = P[g_1(x), \dots, g_t(x)]$ ¹⁾. Es wird $\mathfrak{L}$ endlicher Erweiterungskörper des Quotientenkörpers $P(g_1(x), \dots, g_t(x))$ von $\mathfrak{T}$, und der aus allen $\mathfrak{R}$ -ganzen Elementen aus $\mathfrak{L}$ bestehende Ring $\mathfrak{S}$ wird identisch mit dem aller $\mathfrak{T}$ -ganzen Elemente aus $\mathfrak{L}$.

In $\mathfrak{T}$ gilt der Teilerkettensatz für das System aller Ideale und $\mathfrak{T}$ ist ganz abgeschlossen in seinem Quotientenkörper, beides da $\mathfrak{T}$ dem Polynombereich von t Unbestimmten isomorph ist. Aus der Voraussetzung, daß $P^{1/p}$ endlich in bezug auf P , folgt weiter daß $\mathfrak{T}^{1/p}$ endlich in bezug auf $\mathfrak{T}$ ²⁾. Somit gilt in $\mathfrak{S}$ der Teilerkettensatz für das System aller $\mathfrak{T}$ -Moduln — insbesondere besitzt $\mathfrak{S}$ als $\mathfrak{T}$ umfassenden Unterring von $\mathfrak{S}$ eine endliche $\mathfrak{T}$ -Modulbasis ³⁾. Die Existenz der endlichen $\mathfrak{T}$ -Modulbasis für $\mathfrak{S}$ gilt weiter ohne irgend einschränkende Voraussetzung über den Koeffizientenbereich P , wenn $\mathfrak{L}$ Erweiterung erster Art von $P(g_1(x), \dots, g_t(x))$ wird, also insbesondere immer wenn P von der Charakteristik Null ist ³⁾.

Es bedeute $h_1(x), \dots, h_s(x)$ eine $\mathfrak{T}$ -Modulbasis von $\mathfrak{S}$; dann zeigt die Darstellung: $f(x) = A_1(g)h_1(x) + \dots + A_s(g)h_s(x)$ für beliebiges $f(x)$ aus $\mathfrak{S}$ — wo die A als Elemente aus $\mathfrak{T}$ Polynome in den g bedeuten — daß $g_1(x), \dots, g_t(x), h_1(x), \dots, h_s(x)$ die gesuchte Integritätsbasis bilden.

Enthält der Körper P nur endlich viele Elemente, so enthält doch der durch Adjunktion einer Unbestimmten u — d. h. eines in bezug auf $\mathfrak{S}$ transzendenten Elementes — entstandene Körper $P(u)$ unendlich viele Elemente. Also besitzt der Ring $\mathfrak{S}(u)$ eine endliche Integritätsbasis in bezug auf $P(u)$ als Koeffizientenbereich; und da $\mathfrak{S}(u)$ Vereinigungsring von $\mathfrak{S}$ und $P(u)$ ist, kann diese Basis

1) Vergl. Hilbert, Über die vollen Invariantensysteme, § 1. Math. Ann., 42 (1893), S. 313—373.

2) Vergl. die in der Einleitung zitierte Note von Artin-v. d. Waerden.

3) Vergl. etwa E. Noether, Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern, § 3. Math. Ann., 96 (1926), S. 26—61.

— durch Aufspalten nach den Potenzen von u — aus $\mathfrak{S}$ gewählt werden, wobei die Basiselemente g_i von $\mathfrak{T}$ jetzt kein irreduzibles System mehr bilden werden. Damit läßt jedes Polynom $f(x)$ aus $\mathfrak{S}$ eine Darstellung zu: $C(u)f(x) = G(u, g_i, h_i)$, wo $C(u)$ ein von Null verschiedenes Polynom aus $P[u]$ bedeutet und G ganz in u, g_i, h_i wird. Der Vergleich der Koeffizienten einer geeigneten Potenz von u zeigt, daß in $g_i(x)$ und $h_i(x)$ eine Integritätsbasis von $\mathfrak{S}$ gegeben ist. Damit ist das Endlichkeitskriterium allgemein bewiesen.

§ 2. Die Invariantenendlichkeit.

1. Unter einer endlichen linearen Gruppe der Charakteristik p sei verstanden eine Gruppe $\mathfrak{S}$ von h linearen Substitutionen $A_1, \dots, A_h$ (von nicht verschwindender Determinante) mit Koeffizienten aus einem Körper P der Charakteristik p . Dabei sei durch A_k die lineare Substitution

$$x_1^{(k)} = a_{11}^{(k)} x_1 + \dots + a_{1n}^{(k)} x_n, \dots, x_n^{(k)} = a_{n1}^{(k)} x_1 + \dots + a_{nn}^{(k)} x_n$$

oder abkürzend: $(x^{(k)}) = A_k(x)$ dargestellt. Die Gruppe $\mathfrak{S}$ führt also die Reihe (x) mit den Elementen $x_1, \dots, x_n$ über in die Reihen $(x^{(k)})$ mit den Elementen $x_1^{(k)}, \dots, x_n^{(k)}$. Da unter $A_1, \dots, A_h$ 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 verstanden eine solche ganze rationale Funktion von $x_1, \dots, x_n$ — mit Koeffizienten aus P^1), — die bei Anwendung von $A_1, \dots, A_h$ identisch ungeändert bleibt. Zu diesen Invarianten gehören also alle symmetrischen Funktionen — mit Koeffizienten aus P — der Reihen $(x^{(k)})$. Umgekehrt gilt für jede solche Invariante:

$$f(x) = f(x^{(1)}) = \dots = f(x^{(h)}) \quad \text{oder} \quad h \cdot f(x) = f(x^{(1)}) + \dots + f(x^{(h)}).$$

Hieraus folgt, daß für den Fall, wo die Ordnung h der Gruppe nicht durch die Charakteristik teilbar ist — also insbesondere im Fall der Charakteristik Null — die symmetrischen Funktionen

1) Das stellt insofern keine Einschränkung der Allgemeinheit dar, als jede Invariante mit Koeffizienten aus einem Körper der Charakteristik p — der mit P einen gemeinsamen Umfassungskörper besitzen muß, damit die Invarianten definiert sind — sich linear aus endlich vielen Invarianten mit Koeffizienten aus P zusammensetzen läßt. Man braucht im allgemeinen Fall nur die Koeffizienten durch solche auszudrücken, die in bezug auf P linear unabhängig sind; dann ist die Eigenschaft der Invarianz identisch in diesen unabhängigen erfüllt.

der Reihen $(x^{(k)})$, mit Koeffizienten aus P , auch die Gesamtheit der Invarianten erschöpfen. Da nun diese symmetrischen Funktionen eine endliche Integritätsbasis besitzen, ist in diesem Fall der Endlichkeitsbeweis erbracht; zugleich ergibt sich die Integritätsbasis als das System $G_{\alpha\alpha_1\ldots\alpha_n}(x)$ der Koeffizienten der Galoisschen Resolvente¹⁾:

$$\begin{aligned}\Phi(z, u) &= \Pi(z - u_1 x_1^{(k)} - \cdots - u_n x_n^{(k)}) \\ &= z^h + \Sigma G_{\alpha\alpha_1\ldots\alpha_n}(x) z^\alpha u_1^{\alpha_1} \ldots u_n^{\alpha_n} \quad (\alpha \neq h; \alpha + \alpha_1 + \cdots + \alpha_n = h).\end{aligned}$$

2. Für den Fall, daß h durch p teilbar, braucht nicht notwendig jede Invariante der Gruppe eine symmetrische Funktion der Reihen $(x^{(k)})$ zu sein, da man jetzt von $h \cdot f(x)$ nicht mehr auf $f(x)$ schließen kann. Es bildet aber der aus den endlich vielen Invarianten $G_{\alpha\alpha_1\ldots\alpha_n}(x)$ — den Koeffizienten der Galoisschen Resolvente — abgeleitete Ring $\Re$ einen endlichen Unterring des Systems $\Im$ aller Invarianten, und es ist zu zeigen, daß $\Im$ in bezug auf $\Re$ die Voraussetzungen des Endlichkeitskriteriums erfüllt.

Vorerst kann ohne Beschränkung der Allgemeinheit²⁾ als Koeffizientenbereich der aus allen Substitutionskoeffizienten $a_{\mu\nu}^{(k)}$ abgeleitete Unterkörper $\bar{P}$ von P zugrunde gelegt werden. Dieser aus endlich vielen Elementen abgeleitete Körper entsteht also durch Adjunktion endlich vieler algebraischer oder transzendenter Elemente zum Primkörper; und da der Primkörper vollkommen, so folgt daß $\bar{P}^{1/p}$ endlich in bezug auf $\bar{P}$ ist³⁾.

Es ist weiter zu zeigen, daß $\Im$ algebraisch ganz von $\Re$ abhängt. Nach 1. tritt unter den h Reihen $x^{(k)}$ auch die ursprüngliche $x_1, \ldots, x_n$ auf; also verschwindet die Galoissche Resolvente $\Phi(z, u)$ für $z = u_1 x_1 + \cdots + u_n x_n$ identisch in u . Spezialisiert man jeweils alle u zu Null bis auf u_i , das gleich der Einheit gesetzt wird, so ergibt sich eine Relation:

$$x_i^h + \Sigma x_i^\alpha G_{\alpha 0 0 \ldots \alpha_i \ldots 0 0}(x) = 0 \quad (\alpha \neq h; \alpha + \alpha_i = h),$$

die zeigt, daß jedes x_i algebraisch ganz von $\Re$ abhängt. Damit aber gilt das gleiche für jedes beliebige Polynom in x ; insbesondere hängt also $\Im$ algebraisch ganz von $\Re$ ab. Damit sind die Voraussetzungen des Endlichkeitskriteriums erfüllt, die Invariantenendlichkeit ist bewiesen.

1) Siehe S. 28, Fußnote 1.

2) Siehe S. 33, Fußnote.

3) Siehe S. 32, Fußnote 2.

3. Es sei bemerkt, daß die gleichen Schlüsse die Endlichkeit der Relativ- und der Modularinvarianten ergeben. Ein Polynom $f(x)$ heißt Relativinvariante der Gruppe, wenn alle $f(x^{(k)})$ sich von $f(x)$ nur durch einen von Null verschiedenen Faktor aus $\bar{P}$ unterscheiden. Das System der absoluten Invarianten — insbesondere also der aus den $G_{\alpha\alpha_1\ldots\alpha_n}(x)$ abgeleitete Ring $\mathfrak{R}$ — bildet also einen endlichen Unterring des aus allen Relativinvarianten abgeleiteten Rings; und wie oben sind die Voraussetzungen des Endlichkeitskriteriums in bezug auf $\mathfrak{R}$ erfüllt.

Ein Polynom $f(x)$ heißt Modularinvariante der Gruppe, wenn $f(x)$ gleich $f(x^{(k)})$ wird für jedes spezielle Wertsystem $x_1 = \alpha_1, \ldots, x_n = \alpha_n$ aus $\bar{P}$. Jede absolute Invariante ist zugleich Modularinvariante; wenn aber $\bar{P}$ nur endlich viele Elemente enthält, so braucht des Umgekehrte nicht zu gelten. Auch hier sind die Voraussetzungen des Endlichkeitskriteriums in bezug auf den aus den $G_{\alpha\alpha_1\ldots\alpha_n}(x)$ abgeleiteten Unterring $\mathfrak{R}$ erfüllt.