Ueber die Endlichkeit der Invarianten binärer Formen

R. Weitzenböck (Amsterdam).

Communicated by H. W. Turnbull.

(*Received* 24*th November* 1932. *Read* 20*th January* 1933.)

In der Theorie der Invarianten binärer Formen gilt der Satz, dass die projektiven Komitanten eines vollen Systems durch sukzessives Ueberschieben berechnet werden können. Hierauf beruht der Originalbeweis für die Endlichkeit, den P. Gordan 1868 zuerst gegeben hat.[1] Konstruktiv wird dieser Beweis aber erst dann, wenn man von vorneherein eine obere Grenze für den Grad der Komitanten eines vollen Systems in den Koeffizienten der Grundformen angeben kann. Also eine natürliche Zahl N, die die Sicherheit gibt, dass alle Komitanten eines vollen Systems gefunden sind, wenn man die Ueberschiebungen soweit berechnet hat, dass ihr Grad N nicht übersteigt.

Der Originalbeweis Gordans eignet sich nicht für die Bestimmung einer solchen Schranke. Dagegen ergibt sich aus einem, durch Mertens[2] gegebenen Endlichkeitsbeweis in natürlicher Weise ein Verfahren, das zur Ermittlung von N führt; wir folgen deshalb in unserer Darstellung dem Beweise von Mertens.

Die gefundene Schranke ist nur von theoretischem Werte, da sie viel zu hoch ist; aber es handelt sich ja im Prinzipe nur um die tatsächliche Aufweisung einer endlichen natürlichen Zahl für den allgemeinen Fall. In speziellen Fällen wird sich meist eine viel kleinere Schranke ermitteln lassen.

Da sich die Ermittlung der Invarianten von n-ären Formen bezüglich r-gliedriger linearer Gruppen auf die Berechnung der projektiven Invarianten binärer Formen zurückführen lässt, ist es auch für die erstgenannten Komitanten möglich eine obere Gradschranke anzugeben, worauf ich an anderer Stelle näher eingehen werde.

---

[1] P. Gordan, *Journal für Math.*, **69** (1868), 323-354; vgl. auch: Gordan-Kerschensteiner, *Vorles. über Invariantentheorie* 2, Leipzig (1887), 231.

[2] F. Mertens, *Journal für Math.*, **100** (1887), 223-230, Vgl. auch D. Hilbert, *Math. Annalen*, **33** (1889), 223-226; E. B. Elliot, *Algebra of Quantics*, Oxford (1895), 188; Grace and Young, *The Algebra of Invariants*, Cambridge (1903), 101.

https://doi.org/10.1017/S0013091500007963 Published online by Cambridge University Press

§ 1.

Es sei $\{F\}$ ein System von binären Grundformen, das nicht aus einer einzigen Linearform besteht und das die Form $f_n = a_x^n$ $(n \geqq 1)$ enthält.

(1) $$K(F) = A_1, A_2, \ldots; \; B_1(x), B_2(x), \ldots$$

sei ein kleinstes volles System von ganzen, rationalen, projektiven Komitanten von $\{F\}$: A_ν seien die Invarianten, $B_\nu(x)$ die Kovarianten von $K(F)$.

Wir nennen $N(F)$ die Anzahl der Komitanten (1), $N_c(F)$ den Höchstgrad dieser Komitanten in allen Formenkoeffizienten zusammen und $N_x(F)$ den Höchstgrad in x_1/x_2 bei den Kovarianten $B_\nu(x)$. Es ist dann $N(F) \geqq 2$ und $N_x(F) \geqq n$.

Wir nehmen zu $\{F\}$ die Linearform

(2) $$P = (px) = p_1 x_2 - p_2 x_1$$

als weitere Grundform hinzu. Hierdurch entsteht das Grundformensystem $\{F, P\}$ mit dem vollen System

(3) $$K(F, P) = A_1, A_2, \ldots; \; P; \; Q_1, Q_2, \ldots,$$

wobei die Komitanten Q_i aus den $B_\nu(x)$ durch Polarisieren mit der Reihe p_1/p_2 erhalten werden. Ist also z. B. $B_\nu(x) = a_x^\sigma$, dann sind

(4) $$a_x^\sigma, \; a_x^{\sigma-1} a_p, \; a_x^{\sigma-2} a_p^2, \; \ldots, \; a_p^\sigma$$

unter den Q_i von (3) zu finden.

Für die zum vollen System $K(F, P)$ gehörigen Maximalzahlen finden wir dann nach (4), da aus jedem $B_\nu(x)$ vom Grade σ in den x_i genau σ neue Komitanten Q_i entstehen, $\sigma \leqq N_x(F)$ und die Anzahl der Kovarianten $B_\nu(x)$ kleiner als $N(F)$ ist:

$$N(F, P) = N(F) + 1 + \sum_B \sigma < N(F) + 1 + N(F) \, . \, N_x(F),$$

oder, wenn wir kurz N, N_x und N_c für $N(F)$, $N_x(F)$ und $N_c(F)$ schreiben:

(5a) $$N(F, P) < N \, . \, (1 + N_x)$$

(5b) $$N_x(F, P) = N_x.$$

Bei der Bestimmung von $N_c(F, P)$ sind die p_i als Formenkoeffizienten zu betrachten; da die $Q_i(x)$ höchstens vom Grade N_x in den p_i werden, haben wir

(5c) $$N_c(F, P) \leqq N_x + N_c.$$

Wir betrachten jetzt alle Komitanten G von $\{F, P\}$, die in den p_i und in den Koeffizienten $a_{ikl\ldots}$ von $f_n = a_x^n$ von *gleichem Grade* $(\geqq 0)$

https://doi.org/10.1017/S0013091500007963 Published online by Cambridge University Press

sind und beweisen nach MERTENS, dass alle diese G einen *endlichen Integritätsbereich* bilden.

Wir verteilen die in (3) stehenden Polynome von $K(F, P)$ in drei Klassen S_i:

(6) $S_1 = P_1, P_2, .., P_\nu$; $S_2 = P_{\nu+1}, P_{\nu+2}, .., P_\rho$ und $S_3 = R_1, R_2, .., R_\sigma$.

Zu S_1 rechnen wir diejenigen ν Basiskomitanten P_i von $K(F, P)$, bei denen die Differenz: Grad in den Koeffizienten von $\{F\}$ vermindert um den Grad in p_i, eine positive ganze Zahl $a_i > 0$ ist; zu S_2 rechnen wir diejenigen, bei denen diese Differenz gleich Null und zu S_3 schliesslich die, bei denen diese Differenz $= -b_\kappa < 0$ wird. Für die Zahlen ν und σ haben wir dann neben $\nu < \rho$:

$$N(F) \leqq \nu < N(F, P) - 1 \text{ und } 1 \leqq \sigma < N(F, P) - N(F),$$

also nach (5a):

(7) $$N \leqq \nu < N . (N_x + 1) \text{ und } 1 \leqq \sigma < N . N_x.$$

Jede Komitante G aus $K(F, P)$ zerfällt jetzt nach (6) in Glieder der Gestalt

$$G = P_1^{a_1} P_2^{a_2} \ldots . P_\nu^{a_\nu} \ldots . P_\rho^{a_\rho} R_1^{\beta_1} R_2^{\beta_2} \ldots . R_\sigma^{\beta_\sigma}$$

wobei die Exponenten einer Gleichung genügen:

(8) $$a_1 \alpha_1 + a_2 \alpha_2 + \ldots . + a_\nu \alpha_\nu = b_1 \beta_1 + b_2 \beta_2 + \ldots . + b_\sigma \beta_\sigma.$$

Hier betrachten wir die ganzen, nicht-negativen Zahlen a_i und b_k als gegebene Koeffizienten, die α_r und β_s hingegen als ganzzahlige Unbekannte $\geqq 0$. (8) hat dann eine endliche Lösungsbasis und deren τ Basislösungen erhält man nach MERTENS wie folgt. Ist t_{ik} der grösste gemeinsame Teiler von a_i und b_k, dann bilden

(9) $$\alpha_i = \frac{b_\kappa}{t_{i\kappa}}, \quad \beta = \frac{a_i}{t_{i\kappa}},$$

alle anderen α_r und β_s gleich Null eine Basislösung von (8) und es gibt $\tau_1 = \nu\sigma$ solche Lösungen. Neben diesen kann es noch τ_2 weitere Basislösungen geben, bei denen die linke Seite von (8) höchstens gleich der Zahl

(10) $$s = \sum_{i=1}^{\nu} \sum_{\kappa=1}^{\sigma} \frac{a_i b}{t_{i\kappa}} - \nu\sigma$$

ist.

Wegen

$$s \leqq \left(\sum_{i=1}^{\nu} a_i\right) . \left(\sum_{\kappa=1}^{\sigma} b_\kappa\right) - \nu\sigma \leqq \nu\,(a_i)_{\max.} . \sigma\,(b_\kappa)_{\max.} - \nu\sigma$$
$$\leqq \nu\sigma\,[N_c(F) . N_x(F) - 1]$$

wird nach (7):

https://doi.org/10.1017/S0013091500007963 Published online by Cambridge University Press

(11) $$s < N^2 N_x (N_x + 1)(N_c N_x - 1) = S.$$

Es gilt also für diese τ_2 weiteren Basislösungen:

$$a_1 \alpha_1 + a_2 \alpha_2 + \ldots . + a_\nu \alpha_\nu < S;$$

hieraus folgt wegen $a_i \geqq 1$:

$$\alpha_i < S, \quad \beta_\kappa < S$$

und also $\tau_2 <$ als die grössere der Zahlen S^ν, S^σ, somit wieder nach (7):

$$\tau_2 < S^{N(N_x+1)}.$$

Daher ergibt sich für die Anzahl $\tau_1 + \tau_2$ der Basislösungen.

$$\tau = \tau_1 + \tau_2 < \nu\sigma + S^{N(N_x+1)},$$

d. h. nach (7) und (11):

(12) $$\tau < N^2 N_x (N_x + 1) + [N^2 N_x (N_x + 1)(N_c N_x - 1)]^{N(N_x+1)}.$$

Die mit diesen τ Basislösungen gebildeten Komitanten

(13) $$G = P_1^{\alpha_1} P_2^{\alpha_2} \ldots . P_\nu^{\alpha_\nu} R_1^{\beta_1} R_2^{\beta_2} \ldots . R_\sigma^{\beta_\sigma}$$

bilden mit den $\rho - \nu$ Komitanten $P_{\nu+1}, \ldots ., P_\rho$ von (6) zusammen eine Integritätsbasis $G_1, G_2, \ldots ., G_\gamma$ für alle G. Da $\rho \leqq N(F, P) - 1$ ist, folgt nach (5a):

$$\rho - \nu \leqq N(F, P) - 2 \leqq N(N + 1) - 1.$$

Für die Anzahl γ der Basiskomitanten G_i ergibt sich also:

(14) $$\gamma = \tau + \rho - \nu$$
$$< N(N_x + 1) - 1 + N^2 N_x (N_x + 1) + [N^2 N_x (N_x + 1)(N_c N_x - 1)]^{N(N_x+1)}.$$

Für die Gradzahlen der Komitanten (6) gelten (5b) und (5c). Nach (13) haben wir daher für den Grad γ_x von G_i in den x_1/x_2:

$$\gamma_x \leqq \left(\sum_{i=1}^{\nu} \alpha_i + \sum_{\kappa=1}^{\sigma} \beta_\kappa\right) . N_x (F, P)$$
$$< (\nu + \sigma) . S . N_x,$$

also nach (7) und (11):

(15) $$\gamma_x < N^3 N_x^2 (2N_x + 1)(N_x + 1)(N_x N_c - 1).$$

Auf dieselbe Weise erhalten wir für den Grad γ_c der Basiskomitanten G_i in den Koeffizienten der Formen $\{F, P\}$:

$$\gamma_c \leqq \left(\sum_{i=1}^{\nu} \alpha_i + \sum_{\kappa=1}^{\sigma} \beta_\kappa\right) . N_c (F, P)$$
$$< (\nu + \sigma) . S . (N_x + N_c),$$

(16) $$\gamma_c < N^3 N_x (N_x + 1)(2N_x + 1)(N_x + N_c)(N_x N_c - 1).$$

https://doi.org/10.1017/S0013091500007963 Published online by Cambridge University Press

§ 2.

Es sei nun $\{F'\}$ das System binärer Grundformen, das aus $\{F\}$ entsteht, wenn man die Form $f_n = a_x^n$ ersetzt durch eine Form $(n+1)$-ten Grades $f_{n+1} = A_x^{n+1}$ und die übrigen Grundformen ungeändert lässt. Ist dann H eine Komitante des Systems $\{F'\}$, in der die Koeffizienten von f_{n+1} wirklich auftreten, und ersetzt man diese Koeffizienten von f_{n+1} durch die entsprechenden des Produktes $f_n . P$, so entsteht aus H eine Komitante G'' von $\{F, P\}$, die in den Koeffizienten von f_n und in den p_1/p_2 vom selben Grade ist. G'' ist daher durch die $G_1, G_2, \ldots, G_\gamma$ des vorigen Abschnitt ganz und rational ausdrückbar, d. h. wird eine Summe von Potenzprodukten

$$(17) \qquad \Theta = G_1^{\mu_1} G_2^{\mu_2} \ldots G_\gamma^{\mu_\gamma}.$$

Jetzt führen wir n Linearformen

$$(18) \qquad Q = q_1 x_2 - q_2 x_1, \quad R = r_1 x_2 - r_2 x_1, \ \ldots, \ S = s_1 x_2 - s_2 x_1$$

ein und ersetzen in jedem G_i die Koeffizienten von f_n durch die entsprechenden der Produktform $Q . R \ldots . S$. Hierdurch entstehen aus den G_i Formen G_{i1}, die symmetrisch in den n Reihen $q_i, r_i, \ldots, s_i$ sind; aus Θ entsteht ein Θ_1 und aus G'' entsteht eine Form

$$(19) \qquad G_1'' = \Sigma\, G_{11}^{\mu_1} G_{21}^{\mu_2} \ldots G_{\gamma 1}^{\mu_\gamma},$$

die symmetrisch ist in allen $n+1$ *Reihen* $p, q, r, \ldots, s$. Hieraus folgt, dass wir eindeutig von G_1'' zum ursprünglichen H zurückgelangen, wenn wir in G_1'' jedes Produkt $p_i q_k r_l \ldots$ durch den Koeffizienten $A_{ikl\ldots}$ von f_{n+1} ersetzen.

In (19) vertauschen wir zuerst die p_i mit den q_i; dies gibt

$$G_1'' = \Sigma\, G_{12}^{\mu_1} G_{22}^{\mu_2} \ldots G_{\gamma 2}^{\mu_\gamma};$$

dann die p_i mit den r_i:

$$G_1'' = \Sigma\, G_{13}^{\mu_1} G_{23}^{\mu_2} \ldots G_{\gamma 3}^{\mu_\gamma},$$

u. s. f.; zum Schlusse die p_i mit den s_i. Alles addiert gibt:

$$(20) \qquad (n+1) . G_1'' = \Sigma\, G_{11}^{\mu_1} \ldots G_{\gamma 1}^{\mu_\gamma} + \Sigma\, G_{12}^{\mu_1} \ldots G_{\gamma 2}^{\mu_\gamma} + \ldots + \Sigma\, G_{1, n+1}^{\mu_1} \ldots G_{\gamma, n+1}^{\mu_\gamma}.$$

Gehen wir jetzt aus von

$$(21) \qquad S_m = (u_1 G_{11} + \ldots + u_\gamma G_{\gamma 1})^m + (u_1 G_{12} + \ldots + u_\gamma G_{\gamma 2})^m \\ + \ldots + (u_1 G_{1, n+1} + \ldots u_\gamma G_{\gamma, n+1})^m,$$

dann ist in S_m der Koeffizient von $u_1^{\mu_1} u_2^{\mu_2} \ldots u_\gamma^{\mu_\gamma}$ bis auf einen Zahlenfaktor gleich dem G_1'' von (20) mit $\mu_1 + \mu_2 + \ldots + \mu_\gamma = m$. Nun ist

https://doi.org/10.1017/S0013091500007963 Published online by Cambridge University Press

jedes S_m ganz und rational durch diejenigen Polynome G_1'' auszudrücken, für welche

(22) $$\mu_1 + \mu_2 + \ldots. + \mu_\gamma \leqq n + 1$$

wird. Wir haben also als Integritätsbasis aller G_1'' eine endliche Anzahl π von Polynomen

(23) $$G''_{1,\alpha} = \sum_i G_{1i}^{\alpha_1} G_{2i}^{\alpha_2} \ldots. G_{\gamma i}^{\alpha_\gamma} \qquad (\alpha_1 + \alpha_2 + \ldots. + \alpha_\gamma \leqq n + 1)$$

und wenn wir in diesen $p_i q_k r_l \ldots. = A_{ikl\ldots.}$ setzen, erhalten wir eine Integritätsbasis für alle Komitanten H. Die Anzahl π dieser Basiskomitanten H ist dann höchstens gleich der Zahl der Koeffizienten aller Potenzprodukte $u_1^{\alpha_1} u_2^{\alpha_2} \ldots. u_\gamma^{\alpha_\gamma}$ in $S_1, S_2, \ldots., S_{n+1}$, also, da S_m genau $\binom{\gamma + m - 1}{m}$ Koeffizienten enthält:

$$\pi \leqq \binom{\gamma}{1} + \binom{\gamma+1}{2} + \ldots. + \binom{\gamma+n}{n+1} = \binom{\gamma+n+1}{n+1}.$$

Somit gilt für die Anzahl der Basiskomitanten von $\{F'\}$:

(24) $$N(F') \leqq \binom{\gamma+n+1}{n+1} + N(F, P)$$

wobei für γ die Ungleichung (14) und für $N(F, P)$ die Ungleichung (5a) gilt.

Weiters haben wir für den Grad γ''_x der Komitanten $G''_{1,\alpha}$ von (23):

$$\gamma''_x \leqq (\alpha_1 + \alpha_2 + \ldots. + \alpha_\gamma) \cdot \gamma_x \leqq (n + 1)\, \gamma_x.$$

Daher ist $N_x(F')$ höchstens gleich der grösseren der Zahlen $(n + 1)\,\gamma_x$ und $N_x(F, P) = N_x$, also nach (15):

(25) $$N_x(F') < (n + 1)\, N^3 N_x (2N_x + 1)(N_x + 1)(N_x N_c - 1).$$

Auf dieselbe Art erhält man nach (16):

(26) $$N_c(F') < (n + 1)\, N^3 N_x (2N_x + 1)(N_x + 1)(N_x + N_c)(N_x N_c - 1).$$

Hiemit haben wir für $N(F')$, $N_x(F')$ und $N_c(F')$ obere Schranken gefunden, die nur von n und den Zahlen $N(F)$, $N_x(F)$ und $N_c(F)$ des Grundformensystems $\{F\}$ abhängen. Ist $n \geqq 2$, dann kann man die letzten drei Zahlen wieder abschätzen, ausgehend von einem Grundformensystem $\{F^{(-1)}\}$, das aus $\{F\}$ entsteht, wenn f_n durch f_{n-1} ersetzt wird u. s. f. Schliesslich gelangt man zu einem System $\{L\}$ von binären Linearformen $L_1, L_2, \ldots., L_j$ $(j \geqq 2)$ und für dieses gilt:

(27) $$N(L) = j + \tfrac{1}{2} j\,(j - 1), \quad N_x(L) = 1, \quad N_c(L) = 2.$$

https://doi.org/10.1017/S0013091500007963 Published online by Cambridge University Press

§ 3.

Um einfachere Ausdrücke zu erhalten, vergrössern wir jetzt die gefundenen Schranken nach oben. Nennen wir M die grösste der drei Zahlen $N(F)$, $N_x(F)$ und $N_c(F)$ und schliessen den Fall aus, dass $\{F\}$ aus einer einzigen binären qudratischen Form besteht, so können wir $n+1 \leqq M$ und $M \geqq 3$ voraussetzen.

Nach (14) haben wir dann

$$\gamma < M(M+1) + M^3(M+1) + [M^3(M+1)M^2]^{M(M+1)};$$

da $M+1 \leqq \frac{4}{3} M$ und $M^2+1 \leqq \frac{10}{9} M^2$ ist, wird dies zu

$$\begin{aligned} \gamma &< \frac{4}{3} M^2 + \frac{4}{3} M^4 + \left(\frac{4}{3} M^6\right)^{\frac{4}{3}M^2} \\ &< \frac{40}{27} M^4 + M^{8M^2}\left(\frac{4}{3}\right)^{\frac{4}{3}M^2} < M^5 + M^{8M^2+\frac{2}{3}M^2} \\ &< 2M^{8\frac{2}{3}M^2} = M^{8\frac{2}{3}M^2+\log 2/\log M}, \end{aligned}$$

also

(28) $$\gamma < M^{9M^2}.$$

Nach (24) und (5a) ergibt sich

$$\begin{aligned} N(F') &\leqq \frac{\gamma+n+1}{n+1} \cdot \frac{\gamma+n}{n} \cdots \frac{\gamma+1}{1} + M(M+1) \\ &< (\gamma+1)^{n+1} + \frac{4}{3} M^2 \\ &< (1+M^{9M^2})^M + \frac{4}{3} M^2 \\ &< 2(2M^{9M^2})^M, \end{aligned}$$

(29) $$N(F') < M^{10M^3}.$$

In ähnlicher Weise folgen aus (25) und (26):

(30) $$N_x(F') < \frac{32}{9} M^{11} \quad \text{und} \quad N_c(F') < \frac{64}{9} M^{10}.$$

Schreiben wir jetzt M_n statt M und nennen M_{n+1} die grösste der drei Zahlen $N(F')$, $N_x(F')$ und $N_c(F')$, so folgt:

(31) $$M_{n+1} < (M_n)^{10M_n^3}.$$

Führen wir eine Funktion ϕ ein durch

(32) $$\phi(a) = \phi_1(a) = a^{10a^3}$$

und setzen

$$\phi_2(a) = \phi(\phi(a)), \quad \phi_3(a) = \phi(\phi_2(a)), \; \ldots,$$

so können wir nach (31) schreiben:

(33) $$M_n < \phi_1(M_{n-1}) < \phi_2(M_{n-2}) < \cdots < \phi_k(M_{n-k}).$$

https://doi.org/10.1017/S0013091500007963 Published online by Cambridge University Press

Sei nun ein System $\{F\}$ von $s \geqq 1$ Grundformen

$$f_{n_1},\ f_{n_2},\ \ldots ,\ f_{n_s}$$

der Grade $n_1, n_2, \ldots, n_s$ in x_1/x_2 gegeben und wenigstens ein $n_i \geqq 2$. Dann ist

$$M(F) < \phi(M(F_1)),$$

wo $\{F_1\}$ aus $\{F\}$ entsteht, wenn f_{n_i} durch eine Grundform f_{n_i-1} ersetzt wird. Ebenso ist

$$M(F_1) < \phi(M(F_2))$$

wo $\{F_2\}$ aus $\{F_1\}$ entsteht, indem man entweder f_{n_i-1} durch eine f_{n_i-2} oder eine f_{n_k} durch eine f_{n_k-1} ersetzt. Setzen wir also

$$d = n_1 + n_2 + \ldots + n_s - s, \tag{34}$$

so sind wir für $s > 1$ nach d Schritten bei einem System $\{L\}$ von Linearformen angelangt, wofür also

$$M(L) = s + \binom{s}{2} < s^2$$

ist. Wenn aber $s = 1$ und $n_1 \geqq 2$ ist, so sind wir nach $d - 1 = n_1 - 2$ Schritten bei einer binären quadratischen Form mit $M = 2$ angelangt. In allen diesen Fällen ist

$$M(F) < \phi_d(s^2 + 1).$$

Lassen wir jetzt auch den Fall zu, dass $\{F\}$ nur Linearformen enthält, dann ist $d + 1 = 1$ und

$$M(F) < \phi_{d+1}(s^2 + 1),$$

d. h. wir haben in allen Fällen

$$M(F) < \phi_{d+1}(s^2 + 1). \tag{35}$$

Dies gibt den SATZ:

Ist $f_{n_1}, f_{n_2}, \ldots, f_{n_s}$ ein System von s binären Grundformen der Grade $n_1, n_2, \ldots, n_s$, und ist $K_1, K_2, \ldots, K_m$ ein volles System von projektiven Komitanten dieser Grundformen, so ist die Anzahl m dieser K_i, der Grad eines K_i in den $x_1 : x_2$ und der Grad eines K_i in den Koeffizienten der Grundformen

$$< \phi_{d+1}(s^2 + 1),$$

wo $d = n_1 + n_2 + \ldots + n_s - s$ ist und $\phi_{d+1}(a)$ die $(d+1)$-fach iterierte Funktion

$$\phi(a) = a^{10a^3}$$

bedeutet.

https://doi.org/10.1017/S0013091500007963 Published online by Cambridge University Press