Sitzungsberichte

der

mathematisch-naturwissenschaftlichen Abteilung

der

Bayerischen Akademie der Wissenschaften zu München

1931. Heft III
November-Dezember-Sitzung

München 1932
Verlag der Bayerischen Akademie der Wissenschaften
in Kommission bei der C. H. Beck'schen Verlagsbuchhandlung

Ein Beweis für die Unmöglichkeit einer nicht linearen Korrespondenz zwischen doppelpunktfreien Kurven gleicher Ordnung $n > 3$.

Von H. Kapferer in Freiburg i. Br.

Einleitung.

Der Anlaß zu der vorliegenden Abhandlung war im Grunde ein Problem der Diophantischen Gleichungen. Es gelingt bekanntlich häufig, aus einer gegebenen, etwa zufällig aufgefundenen Lösung einer Diophantischen Gleichung noch unendlich viele weitere Lösungen auf rein algebraischem Wege abzuleiten. Wenn man z. B. die Abhandlungen von L. Euler, der sich mit besonderer Liebe und größtem Erfolg solchen Problemen gewidmet hat, daraufhin untersucht, so kann man feststellen, daß es sich um rationale Transformationen der gegebenen Gleichungen handelt, und zwar, wenn man von den Gleichungen 1. und 2. Grades absieht, stets um nicht lineare Transformationen. Als Beispiel sei die homogene Gleichung

$$x^3 + y^3 + z^3 = 0 \tag{1}$$

genannt. Dieselbe besitzt zwar keine Lösung in von 0 verschiedenen ganzen Zahlen, gestattet aber in übersichtlicher Weise das zu erklären, worauf es hier ankommt. Jedesmal nämlich, wenn die Gleichung (1) von einem Zahlentripel x, y, z aus einem beliebigen Zahlkörper befriedigt wird, so ist auch

$$f^3 + g^3 + h^3 = 0$$

$$\text{für } f = x \cdot (y^3 - z^3);\ g = y \cdot (z^3 - x^3);\ h = z \cdot (x^3 - y^3). \tag{2}$$

Durch Iteration kann man so unendlich viele weitere Zahlentripel finden, welche die Gleichung (1) befriedigen und dem durch x, y, z bestimmten Zahlkörper angehören, und zwar sind diese Tripel alle wesentlich voneinander verschieden, d. h. keine zwei Lösungen einer solchen endlosen Kette von Lösungen werden einander proportional.[1]

[1] Dies läßt sich rein algebraisch beweisen, was aber hier nicht geschehen soll. Statt dessen verweisen wir auf die tatsächlich ganzzahlig lösbare Glei-

Das Polynom $P(xyz) \equiv f^3 + g^3 + h^3$ verschwindet also jedesmal, wenn das Polynom $A \equiv x^3 + y^3 + z^3$ verschwindet, also muß P durch A teilbar sein. In der Tat ist

$$(3) \quad f^3 + g^3 + h^3 = (x^3 + y^3 + z^3)(x^3 - y^3)(y^3 - z^3)(z^3 - x^3)$$

eine Identität in x, y, z.[1]

Wenn man nun allgemein von einer in x, y, z homogenen Gleichung $A(x, y, z) = 0$ ausgeht, so handelt es sich um die Frage, ob es drei zugehörige Formen f, g, h von unter sich gleicher Ordnung m gibt, so daß die Kongruenz besteht:

$$(4) \qquad A(f, g, h) \equiv 0 \,[A(x, y, z)].$$

Wenn insbesondere $m = 1$, die Transformation also linear ist, so bedeutet die Kongruenz (4) eine Transformation von A in sich selbst. Solche Transformationen, überhaupt birationale Transformationen einer Kurve in sich interessieren uns in vorliegender Abhandlung nicht, infolge einer Eigenschaft, die in einem von Schwarz[2] und Klein stammenden Satz ausgedrückt ist: „Algebraische Kurven von höherem Geschlecht als 1 haben nur endlich viele birationale Transformationen in sich selbst."

---

chung $x^3 + y^3 + 7z^3 = 0$. Die Kongruenz $f^3 + g^3 + 7h^3 \equiv 0 \,[x^3 + y^3 + 7z^3]$ ist hier erfüllt für $f = x(y^3 + 7z^3)$; $g = y(7z^3 - x^3)$; $h = z(x^3 - y^3)$, und liefert aus der kleinsten Lösung $x = 2, y = z = -1$ zunächst $x = 4, y = 5, z = -3$, usw. Man zeigt leicht, daß allgemein der größte gemeinsame Teiler der ganzen Zahlen f, g, h gleich 1 oder 3 ist, wenn $(x, y, z) = 1$ ist, daß also tatsächlich durch Iteration unendlich viele wesentlich verschiedene Lösungen gewonnen werden.

[1] Es ist bemerkenswert, daß sogar der Eubersche Beweis der Unmöglichkeit der Gleichung (1) in rationalen Zahlen wesentlich auf einer Identität der Art (3) beruht. Wenn man nämlich Eubers „kleinere" Lösung, die zu dem bekannten Widerspruch führt, mit x, y, z bezeichnet, so wird die gegebene „größere" Lösung, von der er ausgeht, etwa f, g, h, ganz rational von jener kleineren Lösung abhängig, und zwar so:

$$f = x^9 - y^9 + 6x^6y^3 + 3x^3y^6; \; g = y^9 - x^9 + 6y^6x^3 + 3y^3x^6;$$
$$h = 3xyz(x^6 + x^3y^3 + y^6).$$

Es ist wiederum $f^3 + g^3 + h^3 \equiv 0 \,[x^3 + y^3 + z^3]$.

Die hier angegebenen Transformationsformeln stehen nicht explizite bei Euler, sind aber direkte Folgerungen der Beweisführung in seiner „Vollständigen Anleitung zur Algebra".

[2] H. A. Schwarz, Crelles Journal f. Math. **87** (1875); Abhandlungen II, 285. F. Klein, Über Riemanns Theorie der algebr. Fkt. (1882) S. 64.

Dagegen über nicht lineare und zugleich nicht birationale Transformationen sagt der Schwarz-Kleinsche Satz nichts aus.

Wir wollen die Fragestellung noch etwas verallgemeinern. Dies erweist sich sogar als vorteilhaft für die nachfolgende Beweisführung.

A und B seien zwei beliebige Formen gleicher Ordnung n, eventuell auch miteinander identisch. Beide seien doppelpunktfrei, also auch irreduzibel. Es ist die Frage, ob es drei Formen f, g, h der Ordnung m gibt, so daß die Kongruenz besteht:

$$A(f, g, h) \equiv 0 \,[B(x, y, z)]. \tag{5}$$

Dabei sollen f, g, h „wesentlich" nicht linear sein, das soll heißen, das Tripel f, g, h soll keinem linearen und auch keinem konstanten Tripel „aequivalent" sein. Wir bezeichnen allgemein im folgenden zwei Tripel f, g, h und f', g', h' als äquivalent zueinander, wenn es zwei zu B prime Formen t, t' gibt, so daß modulo B die Kongruenzen bestehen:

$$tf \equiv t'f'\,;\; tg \equiv t'g'\,;\; th \equiv t'h'.$$

Das Ziel der vorliegenden Abhandlung ist nichts anderes als der Beweis der Tatsache:

Es ist notwendig n kleiner als 4.

Das ist dann zugleich die genaue Grenze, wie das obige Beispiel für $n = 3$ zeigt.[1]

In der Sprache der algebraischen Geometrie bedeutet die Kongruenz (5) eine Punktkorrespondenz zwischen den Kurven $A = 0$ und $B = 0$, insofern als jeder Nullstelle π von $B(x, y, z)$ eine Nullstelle von $A(x, y, z)$ entspricht, nämlich diese: $x = f(\pi)$; $y = g(\pi)$; $z = h(\pi)$. Unser Hauptsatz behauptet also die Un-

[1] Es ist für eine spätere Stelle (§ 5) nützlich zu wissen, daß wenn A die in (5) ausgedrückte Eigenschaft hat, auch jede Form A', welche aus A durch eine homogene lineare umkehrbare Transformation hervorgeht, die analoge Eigenschaft hat, nämlich:

$$A'(f', g', h') \equiv 0 \,[B].$$

Dabei sind f', g', h' gewisse linear homogene Ausdrücke in f, g, h. Auch ist das Tripel f', g', h' in dem oben genannten Sinn „wesentlich" nicht linear dann und nur dann, wenn Tripel f, g, h wesentlich nicht linear ist.

möglichkeit einer nicht linearen Korrespondenz[1] zwischen doppelpunktfreien Kurven gleicher Ordnung $n > 3$.

§ 1. Formale Folgerungen aus der Kongruenz $A(f, g, h) \equiv 0\ [B]$.

Zunächst eine abkürzende Bezeichnung für 2- und 3-reihige Funktionaldeterminanten: Wenn P, Q, R irgendwelche Formen sind, so sei

$$\begin{vmatrix} \frac{\partial P}{\partial x}, & \frac{\partial P}{\partial y} \\ \frac{\partial Q}{\partial x}, & \frac{\partial Q}{\partial y} \end{vmatrix} = \binom{P, Q}{x, y} \text{ und } \begin{vmatrix} \frac{\partial P}{\partial x}, & \frac{\partial P}{\partial y}, & \frac{\partial P}{\partial z} \\ \frac{\partial Q}{\partial x}, & \frac{\partial Q}{\partial y}, & \frac{\partial Q}{\partial z} \\ \frac{\partial R}{\partial x}, & \frac{\partial R}{\partial y}, & \frac{\partial R}{\partial z} \end{vmatrix} = \binom{P, Q, R}{x, y, z}$$

Falls $P = P_1 \cdot P_2$ ist, so folgt leicht

$$\binom{P, Q}{x, y} = P_1 \binom{P_2, Q}{x, y} + P_2 \binom{P_1, Q}{x, y}$$

und daher, falls $P \equiv 0\ [Q]$ ist, $\binom{P, Q}{x, y} = 0\ [Q]$.

Die Anwendung auf die Identität

$$A(f, g, h) = B \cdot C = D$$

liefert

$$(6) \qquad \binom{D, B}{x, y} \equiv 0\ [B]; \binom{D, B}{y, z} \equiv 0\ [B]; \binom{D, B}{z, x} \equiv 0\ [B].$$

Wir führen folgende Bezeichnungen ein:

$$\frac{\partial A(x, y, z)}{\partial x} = u(x, y, z); \frac{\partial A}{\partial y} = v(x, y, z); \frac{\partial A}{\partial z} = w(x, y, z);$$

$$u(f, g, h) = U(x, y, z); v(f, g, h) = V(x, y, z); w(f, g, h) = W(x, y, z).$$

---

[1] Es gibt einen interessanten Satz von H. Weber (Crelle **96**, 1873), der in Pascals Repertorium II_1 S. 343 so zitiert wird: „Eine Korrespondenz zwischen zwei Kurven von demselben Geschlecht $p > 1$, welche einseitig eindeutig ist, ist auch wechselseitig eindeutig, d. h. birational." Könnte man beweisen, daß sie nicht nur birational, sondern sogar linear ist, so wäre unser Hauptsatz in dem so erweiterten Weberschen Satz enthalten.

Webers Methode ist funktionentheoretisch und benützt Riemannsche Überlegungen. Die vorliegende Abhandlung ist rein algebraisch, wie es auch gegenüber einem Satz, der nur von Identitäten zwischen Polynomen handelt, angemessen erscheint.

Dadurch wird
$$D_x = U \cdot f_x + V \cdot g_x + W \cdot h_x$$
$$D_y = U \cdot f_y + V \cdot g_y + W \cdot h_y$$
$$D_z = U \cdot f_z + V \cdot g_z + W \cdot h_z.$$

Auf diese Weise entstehen aus (6), bei geeigneter Umordnung, die folgenden Kongruenzen:

$$(7)\quad \begin{aligned} U\binom{f,B}{x,y} + V\binom{g,B}{x,y} + W\binom{h,B}{x,y} &\equiv 0\,[B] \\ U\binom{f,B}{y,z} + V\binom{g,B}{y,z} + W\binom{h,B}{y,z} &\equiv 0\,[B] \\ U\binom{f,B}{z,x} + V\binom{g,B}{z,x} + W\binom{h,B}{z,x} &\equiv 0\,[B]. \end{aligned}$$

Wir eliminieren U aus den beiden ersten Kongruenzen (7) und erhalten:

$$(8)\quad \begin{aligned} V \cdot \left\{\binom{g,B}{x,y}\binom{f,B}{y,z} - \binom{g,B}{y,z}\binom{f,B}{x,y}\right\} \\ + W \cdot \left\{\binom{h,B}{x,y}\binom{f,B}{y,z} - \binom{h,B}{y,z}\binom{f,B}{x,y}\right\} \equiv 0\,[B]. \end{aligned}$$

Man beachte, daß die drei Gleichungen (7) durch zyklische Vertauschungen (x, y, z und f, g, h und U, V, W) aus einander hervorgehen. Ebendieselben Vertauschungen müssen daher aus der aus (7) abgeleiteten Kongruenz (8) zwei weitere richtige Kongruenzen liefern. Bevor wir letztere anschreiben, führen wir ein:

$$\binom{g,B}{x,y}\binom{f,B}{y,z} - \binom{g,B}{y,z}\binom{f,B}{x,y} = K_{f,g,B}.$$

Dadurch erhalten wir aus (8):

$$(9)\quad \begin{aligned} V \cdot K_{f,g,B} - W \cdot K_{h,f,B} &\equiv 0\,[B] \\ W \cdot K_{g,h,B} - U \cdot K_{f,g,B} &\equiv 0\,[B] \\ U \cdot K_{h,f,B} - V \cdot K_{g,h,B} &\equiv 0\,[B]. \end{aligned}$$

Zwischen dem Symbol $K_{f,g,B}$ und dem Symbol für Funktionaldeterminanten bestehen nun folgende (leicht verifizierbare) Relationen:

$$K_{f,g,B} = -B_y \cdot \binom{f,g,B}{x,y,z}$$
$$K_{g,h,B} = -B_y \cdot \binom{g,h,B}{x,y,z}$$
$$K_{h,f,B} = -B_y \cdot \binom{h,f,B}{x,y,z}.$$

Dadurch tritt B_y in jeder der Kongruenzen (9) als Faktor heraus, kann aber ohne Störung der Kongruenzen modulo B weggelassen werden, weil ja B irreduzibel, also a fortiori zu B_y teilerfremd ist; es sei denn, daß B_y identisch verschwindet, also y in B gar nicht vorkommt. Aber auch dieser Fall kann vermieden werden durch geeignete Bezeichnung der Variabeln.

So erhält man aus (9) die nachstehenden Kongruenzen, auf denen sich alles Folgende aufbaut:

$$\begin{aligned} V\binom{f,g,B}{x,y,z} - W\binom{h,f,B}{x,y,z} &\equiv 0\,[B] \\ W\binom{g,h,B}{x,y,z} - U\binom{f,g,B}{x,y,z} &\equiv 0\,[B] \\ U\binom{h,f,B}{x,y,z} - V\binom{g,h,B}{x,y,z} &\equiv 0\,[B]. \end{aligned} \tag{10}$$

§ 2. Multiplizitätsrelationen.

Aus den Kongruenzen (10) folgen gewisse Relationen zwischen Schnittpunktmultiplizitätszahlen. Zu deren Aufstellung benötigen wir nur noch die Ungleichungen (11), (12) und (13).

Behauptung:

$$f \not\equiv 0\,[B];\ g \not\equiv 0\,[B];\ h \not\equiv 0\,[B]. \tag{11}$$

Denn wäre etwa $f \equiv 0\,[B]$, also $A\,(0, g, h) \equiv 0\,[B]$, also[1] eine Binärform in g und h teilbar durch B, also wenigstens ein linearer homogener Ausdruck in g, h teilbar durch B, etwa $g \equiv ch \bmod B$, so wäre f, g h dem konstanten Tripel 0, c, 1 äquivalent, entgegen der Voraussetzung des Hauptsatzes.

Wir behaupten ferner:

$$\binom{f,g,B}{x,y,z} \not\equiv 0\,[B];\ \binom{g,h,B}{x,y,z} \not\equiv 0\,[B];\ \binom{h,f,B}{x,y,z} \not\equiv 0\,[B]. \tag{12}$$

Zum Beweis berufen wir uns auf einen, als Hauptsatz I bezeichneten, Satz einer früheren Abhandlung.[2] Nach diesem Satz

[1] $A\,(cy, y, z)$ kann nicht identisch verschwinden, weil sonst A selbst durch $x - cy$ teilbar, also A reduzibel wäre entgegen der Voraussetzung.

[2] H. Kapferer, Über die Jacobi'sche Kurve eines Systems von drei Kurven und den Begriff „Abhängigkeit" bei Polynomen. Mathematische Zeitschrift, Bd. 34, Januar 1932.

ist nämlich $\begin{pmatrix} f, g, B \\ x, y, z \end{pmatrix} \equiv 0\,[B]$ dann und nur dann, wenn es zwei Konstante c_1, c_2 gibt, die nicht beide 0 sind, sodaß $c_1 f \equiv c_2 g \bmod B$, also etwa $f \equiv cg \bmod B$ ist. Dann würde aus

$$A(f, g, h) \equiv A(cg, g, h) \equiv 0\,[B]$$

folgen (vgl. die Anmerkung zu (11)), daß f, g, h einem konstanten Tripel äquivalent wäre.

Wir behaupten schließlich noch:

$$U \not\equiv 0\,[B];\ V \not\equiv 0\,[B];\ W \not\equiv 0\,[B]. \tag{13}$$

Dazu ein Hilfsatz (der auch noch später gebraucht werden wird):

(14) Jede gemeinsame Nullstelle von U, V, W ist zugleich gemeinsame Nullstelle von f, g, h. (Und umgekehrt, weil U, V, W homogen in f, g, h sind.)

Denn sei etwa $x = \alpha$, $y = \beta$, $z = \gamma$ eine gemeinsame Nullstelle von U, V, W, und setzt man

$$f(\alpha, \beta, \gamma) = p;\ \ g(\alpha, \beta, \gamma) = q;\ \ h(\alpha, \beta, \gamma) = r,$$

so folgt, daß die drei Formen A_x, A_y, A_z für $x = p$, $y = q$, $z = r$ gleichzeitig verschwinden. Da aber A nach Voraussetzung keinen Doppelpunkt $\neq (0, 0, 0)$ besitzt, so bleibt nur die Möglichkeit, daß $p = q = r = 0$ ist.

Auf Grund dieses Hilfsatzes (14) folgen nun die drei Ungleichungen (13) so: Wäre eine derselben falsch, so würde aus (10) und (12) folgen, daß alle drei falsch wären. Das System $U \equiv 0\,[B]$, $V \equiv 0\,[B]$, $W \equiv 0\,[B]$ aber würde bedeuten, daß, wegen (14), überhaupt jede Nullstelle von B zugleich gemeinsame Nullstelle von f, g, h wäre; das ist, bei irreduziblem B, nur möglich, wenn Teilbarkeit durch B vorliegt:

$$f \equiv 0\,[B];\ g \equiv 0\,[B];\ h \equiv 0\,[B].$$

Das wäre aber entgegen Satz (11). Somit ist (13) bewiesen.

Die Ungleichungen (12) und (13) gestatten nun, aus dem System (10) folgende Relationen zwischen Schnittpunktmultiplizitätszahlen[1] abzulesen: Für jeden Punkt überhaupt gilt:

---

[1] Die „Multiplizität" eines Punktes in bezug auf zwei teilerfremde Formen $L(x, y, z)$ und $M(x, y, z)$ bezeichnen wir kurz mit (L, M). Wegen der Forderung der Teilerfremdheit mußten wir oben, vor Gebrauch dieses

$$
\begin{aligned}
&(V, B) + \left(\binom{f, g, B}{x, y, z}, B\right) = (W, B) + \left(\binom{h, f, B}{x, y, z}, B\right)\\
(16)\qquad &(W, B) + \left(\binom{g, h, B}{x, y, z}, B\right) = (U, B) + \left(\binom{f, g, B}{x, y, z}, \mathrm{B}\right)\\
&(U, B) + \left(\binom{h, f, B}{x, y, z}, \mathrm{B}\right) = (V, B) + \left(\binom{g, h, B}{x, y, z}, B\right)
\end{aligned}
$$

§ 3. Einige Hilfsätze (allgemeiner Art).

Hilfsatz I.[1] Wenn sämtliche gemeinsamen Nullstellen von zwei teilerfremden Formen $\varphi(x, y, z)$ und $\psi(x, y, z)$ wenigstens in ψ einfache Nullstellen sind, so ist — ψ teilerfremd zu der Form K vorausgesetzt — für die Kongruenz $K \equiv 0\ [\varphi, \psi]$ notwendig und hinreichend, daß auch K diese Nullstellen besitzt, und daß außerdem die Schnittpunktmultiplizität im Kurvenpaar $K = 0$, $\psi = 0$ jeweils mindestens so groß ist wie im Kurvenpaar $\varphi = 0$, $\psi = 0$.

Hilfsatz II.[2] (Eine charakteristische Gleichung für μfache Schnittpunktmultiplizität.)

Symbols, zuerst die Ungleichungen (12) und (13) beweisen. Dieses Symbol befolgt zwei bekannte, im folgenden oft benützte Gesetze, die sich kurz so ausdrücken lassen.

$$(15^a)\qquad (L, N) + (M, N) = (LM, N)$$

$$(15^b)\qquad (L, N) = (L + tN, N),$$

falls die Ordnung von L gleich oder größer als die Ordnung von N, und falls t irgendeine Form, deren Ordnung gleich der Differenz der Ordnungszahlen von L und N ist. Die beiden Relationen (15) sind Folgerungen aus zwei entsprechenden Eigenschaften der allgemeinen Resultante von n Formen mit n Variabeln. Die letzteren findet man z. B. in F. Mertens, Theorie der Elimination, Wiener Akademieberichte **108** (1899), §§ 7 u. 8. Vgl. auch v. d. Waerden, Moderne Algebra II, S. 19, ferner O. Perron, Algebra I. Bd., zweite Auflage, Satz 150 und 151, und H. Kapferer, Axiomatische Begründung des Bézoutschen Satzes. Heidelberger Akademieberichte, 1927.

[1] Entnommen aus H. Kapferer, Notwendige und hinreichende Multiplizitätsbedingungen zum Noetherschen Fundamentalsatz der algebraischen Funktionen. Sitzungsberichte der Heidelberger Akademie, 1927, und H. Kapferer und E. Noether, Mathematische Annalen **97** S. 263.

$K \equiv 0\ [\varphi, \psi]$ soll bedeuten: Es existieren zwei Formen L und M, so daß $K = L\varphi + M\psi$ eine Identität in x, y, z ist.

[2] Entnommen aus H. Kapferer, Über Schnittpunktsysteme mit vorgeschriebenen Multiplizitätszahlen. Sitzungsberichte der Heidelberger Aka-

Wenn $x = \alpha z$, $y = \beta z$ eine gemeinsame Nullstelle von zwei Formen M und B bedeutet, für welche $(M, B) \geqq \mu$ ist, so gibt es zwei weitere Formen T und S, so daß die Kongruenz gilt

$$MT^{\mu} \equiv (x - \alpha z)^{\mu} S \qquad \text{mod } B.$$

Hierbei kann $T = B\ (\alpha z, y, z)$: $y - \beta z$ gewählt werden. Wenn überdies (M, B) genau gleich μ, und wenn $B\ (\alpha z, y, z) \not\equiv 0\ [(y - \beta z)^2]$ ist, so ist $S \neq 0$ im Punkte $x = \alpha z$, $y = \beta z$.[1]

Hilfsatz III.[2] π sei eine gemeinsame Nullstelle der drei Formen L, M, N. Bezüglich π gelte

$$(L, N) \geqq \mu \text{ und } (M, N) \geqq \mu.$$

Ferner sei π speziell in N nur einfache Nullstelle, und die Funktionaldeterminante $I = \begin{pmatrix} L, & M, & N \\ x, & y, & z \end{pmatrix}$ sei zu N teilerfremd. Dann wird behauptet

$$(I, N) \geqq 2\mu.$$

Die beiden folgenden Hilfsätze IV und V sind im wesentlichen Folgerungen aus Hilfsatz II.

Hilfsatz IV. L, M, N seien drei Formen gleicher Ordnung, zu je zwei teilerfremd, mit einer gemeinsamen Nullstelle π. Bezüglich π gelte:

$$(L, N) = \mu;\ (M, N) = \nu;\ \mu \geqq \nu.$$

---

demie, 1930. Der H. II kann übrigens auch, was a. a. O. aus methodischen Gründen nicht geschah, als Folgerung aus H. I angesehen werden.

[1] Zusätze zu Hilfsatz II.

1. Der H. II kann auch so ausgesprochen werden, daß die Rollen von $(x - \alpha z)$ und $(y - \beta z)$ miteinander vertauscht erscheinen. Das ist besonders dann nützlich, wenn es sich um eine Form B mit überhaupt nur einfachen Nullstellen handelt, in welchem Falle stets wenigstens eine der beiden Ungleichungen

$$B\ (\alpha z, y, z) \not\equiv 0\ [(y - \beta z)^2] \text{ und } B\ (x, \beta z, z) \not\equiv 0\ [(x - \alpha z)^2]$$

a priori richtig ist.

2. Die allgemeine Darstellung eines Punktes ist diese $x : y : z = \alpha' : \beta' : \gamma'$ mit $(\alpha', \beta', \gamma') \neq (0, 0, 0)$. Dagegen die Darstellung $x = \alpha z$, $y = \beta z$ setzt $\gamma' \neq 0$, die Darstellung $y = \beta z$, $z = \gamma x$ setzt $\alpha' \neq 0$, die Darstellung $z = \gamma y$, $x = \alpha y$ setzt $\beta' \neq 0$ voraus. Es ist nur Sache der Bezeichnung, den Inhalt des H. II für einen bestimmten dieser drei Fälle richtig auszusprechen.

[2] Entnommen aus H. Kapferer, Über die Jacobi'sche Kurve eines Systems von drei Kurven und den Begriff „Abhängigkeit" bei Polynomen. Mathematische Zeitschrift Bd. 34, Januar 1932, S. 562.

π sei einfache Nullstelle der irreduziblen Form N. Es wird behauptet:

a) Die Summe $L + M$ ist teilerfremd zu N,

b) $(L + M, N) \geqq \nu$ in bezug auf π,

und zwar gewiß Gleichheit, falls $\mu > \nu$ ist.

Beweis: π sei erklärt durch $x = \alpha z$, $y = \beta z$. Dann bestehen nach H. II folgende Identitäten:

$$LT^\nu = (x - \alpha z)^\nu L_1 + L_2 N,$$
$$MT^\nu = (x - \alpha z)^\nu M_1 + M_2 N,$$

(17) also $(L + M) T^\nu = (x - \alpha z)^\nu (L_1 + M_1) + (L_2 + M_2) N$.

Wegen $T \not\equiv 0$ in π und $(M, N) = \nu$ muß auch $M_1 \not\equiv 0$ in π sein. Dagegen ist, falls $\mu > \nu$ ist, $L_1 \equiv 0$ in π wegen $(L, N) > \nu$. Daher kann die Summe $L_1 + M_1$ nicht durch N teilbar sein. Aber auch $x - \alpha z$ kann nicht durch N teilbar sein, weil sonst, entgegen der Voraussetzung, $N(\alpha z, y, z) \equiv 0 [(y - \beta z)^2]$ wäre.[1] Daher folgt aus (17), daß auch $L + M$ nicht durch N teilbar, also teilerfremd zu der irreduziblen Form N ist. Somit folgt weiter aus (17) und (15):

$$(L + M, N) \geqq \nu,$$

und zwar Gleichheit, falls $\mu > \nu$ ist (q. e. d.).

Hilfsatz V. (Ein „transitives" Gesetz für die Multiplizitätszahlen.) L, M, N seien drei Formen mit einer gemeinsamen Nullstelle π; je zwei seien teilerfremd. Bezüglich π gelte

$$(L, N) = \mu \text{ und } (M, N) \geqq \mu.$$

π sei einfache Nullstelle von N. Dann wird behauptet:

$$(L, M) \geqq \mu.$$

Beweis: Für $\mu = 1$ ist der Satz trivial. Für $\mu > 1$ wenden wir H. II an, sowohl auf (L, N) als auch auf (M, N). Wir definieren π so: $x = \alpha z$, $y = \beta z$. Dann wird nach H. II

(18)
$$LT^\mu = (x - \alpha z)^\mu L_1 + L_2 N,$$
$$MT^\mu = (x - \alpha z)^\mu M_1 + M_2 N,$$

wo $T = B(\alpha z, y, z) : (y - \beta z)$ ist. Es ist keine Beschränkung, nach H. II, Zusatz, wenn wir π in der angegebenen Weise de-

[1] Vgl. den Zusatz 1 zu Hilfsatz II.

finieren und außerdem annehmen, daß $T \neq 0$ in π ist. Weiter folgt

$$T^{\mu}\,(LM_2 - ML_2) = (x - \alpha z)^{\mu}\,Q.$$

Da T frei von x ist, so ergibt die Division durch T^{μ}

$$LM_2 - ML_2 = (x - \alpha z)^{\mu}\,R, \tag{19}$$

wo auch R ein homogenes Polynom ist. Wir beweisen H. V zunächst unter der doppelten Voraussetzung, daß

a) jeder Teiler von L im Punkte π verschwindet, und daß

b) $L \not\equiv 0\ [x - \alpha z]$ ist.

Unter diesen beiden Voraussetzungen werden nämlich L und L_2 stets teilerfremd; denn jeder gemeinsame Teiler muß wegen (18) auch L_1 teilen und muß außerdem in π verschwinden. L_1 verschwindet aber nicht in π wegen $(L, N) = \mu$. Daher folgt aus (18)

$$(L_2, L) + (N, L) = \big((x - \alpha z)^{\mu}, L\big) + (L_1, L); \tag{20}$$

andererseits aus (19)

$$(L_2, L) + (M, L) = \big((x - \alpha z)^{\mu}, L\big) + (R, L). \tag{21}$$

Wegen $(L_1, L) = 0$ und $(L, N) = \mu$ ergibt sich schließlich aus (20) und (21)

$$(M, L) = \mu + (R, L)$$

also $$(M, L) \geqq \mu,$$ was zu beweisen war.

Wir haben noch die Einschränkungen a) und b) zu beseitigen: Wenn $\overline{L}$ aus L hervorgeht durch Multiplikation mit irgendwelchen in π nicht verschwindenden Faktoren, so ist

$$(\overline{L}, N) = (L, N) = \mu$$
$$(\overline{L}, M) = (L, M) \geqq \mu.$$

Wenn also H. V unter der Bedingung a) richtig ist, so muß er auch ohne die Einschränkung a) richtig sein.

Es sei ferner $\overline{\overline{L}} = (x - \alpha z)^{\varkappa}\,\overline{L}$, wo $\overline{L}$ die obige Bedeutung hat. Dann ist

$$(\overline{\overline{L}}, N) = \big((x - \alpha z)^{\varkappa}, N\big) + (\overline{L}, N) = \varkappa + (\overline{L}, N)$$
$$(\overline{\overline{L}}, M) = \big((x - \alpha z)^{\varkappa}, M\big) + (\overline{L}, M) \geqq \varkappa + (\overline{L}, M).$$

Schon bewiesen ist: $(\overline{L}, M) \geqq (\overline{L}, N)$, also ergibt sich, daß auch $(\overline{\overline{L}}, M) \geqq (\overline{\overline{L}}, N)$ ist. Somit ist auch die Einschränkung b) beseitigt.

Beispiel zu H. V: $L = x(x-y)$; $M = y^7$; $N = z^4x - y^5$; also $(L, N) = 6$; $(M, N) = 7$; $(L, M) = 14$.

Aus diesem Beispiel geht zugleich hervor, daß H. V falsch würde, wenn man für π eine beliebige vielfache Nullstelle von N zuließe, also etwa M und N miteinander vertauschen würde.

§ 4. Über die gemeinsamen Nullstellen von f, g, h und B.

Die Form B ist nach Voraussetzung frei von vielfachen Nullstellen, also auch irreduzibel. Daher folgt aus (11), daß f, g, h zu B teilerfremd sind. Somit haben die Symbole (f, B), (g, B), (h, B) für jeden Punkt π überhaupt wohl definierte nicht negative ganzzahlige Werte. Wir wollen sagen: Die drei Kurvenpaare:

$$f = 0,\ B = 0;\quad g = 0,\ B = 0;\quad h = 0,\ B = 0$$

haben den Punkt π in der Multiplizität μ gemeinsam, wenn μ die kleinste der drei zu π gehörigen Zahlen (f, B), (g, B), (h, B) bedeutet. μ darf also auch 0 sein. Es seien nun $\pi_1, \pi_2, \ldots, \pi_r$ die gemeinsamen Nullstellen von f, g, h und B; $\mu_1, \mu_2, \ldots, \mu_r$ seien der Reihe nach die zugehörigen Multiplizitätszahlen in dem eben erklärten Sinn, also positive ganze Zahlen. Dann setzen wir zur Abkürzung

$$\sigma = \mu_1 + \mu_2 + \ldots + \mu_r$$

und behaupten — Hilfsatz VI. —

$$\text{Bei } n > 3 \text{ ist stets } \sigma \geqq (m-1)\, n.$$

Daraus folgt a fortiori: $\sigma > 0$ bei jeder nicht linearen Korrespondenz, wegen $m > 1$, daß also f, g, h und B bei $n > 3$ stets wenigstens eine gemeinsame Nullstelle besitzen.

Beweis von H. VI. Es sei π definiert (man beachte die Zusätze zu H. II) durch $x = \alpha z$, $y = \beta z$. Bezüglich π gelte:

$$(f, B) \geqq \mu;\quad (g, B) \geqq \mu;\quad (h, B) \geqq \mu.$$

Für $\mu > 0$ gibt es nach H. II drei weitere Formen S_1, S_2, S_3, welche nachstehende Kongruenzen mod B erfüllen

$$(22)\quad fT^\mu \equiv (x - \alpha z)^\mu S_1;\ gT^\mu \equiv (x-\alpha z)^\mu S_2;\ hT^\mu \equiv (x-\alpha z)^\mu S_3.$$

Hierbei ist $T = B(\alpha z, y, z) : (y - \beta z)$. Für $\mu = 0$ wird (22) trivial richtig. Wenn nun insbesondere μ die kleinste der drei Zah-

len (f, B), (g, B), (h, B), und wenn $T(\alpha, \beta, 1) \neq 0$, d. h. wenn $B(\alpha z, y, z) \not\equiv 0\,[(y - \beta z)^2]$ ist, so wird wenigstens eine der drei Formen $S_1\ S_2\ S_3$ den Punkt π nicht als Nullstelle haben. Aus der Homogenität der Polynome u, v, w und U, V, W folgt jedenfalls

$$(23)\quad \begin{aligned} UT^{n-1} &= u(fT, gT, hT);\ VT^{n-1} = v(fT, gT, hT);\\ WT^{n-1} &= w(fT, gT, hT). \end{aligned}$$

Aus (22) und (23) ergeben sich sofort nachfolgende Kongruenzen mod B:

$$(24)\quad \begin{aligned} UT^{n-1} &\equiv u\left((x - \alpha z)^{\mu} S_1, (x - \alpha z)^{\mu} S_2, (x - \alpha z)^{\mu} S_3\right)\\ &\equiv (x - \alpha z)^{\mu(n-1)}\, u\,(S_1, S_2, S_3)\\ VT^{n-1} &\equiv v\left((x - \alpha z)^{\mu} S_1, (x - \alpha z)^{\mu} S_2, (x - \alpha z)^{\mu} S_3\right)\\ &\equiv (x - \alpha z)^{\mu(n-1)}\, v\,(S_1, S_2, S_3)\\ WT^{n-1} &\equiv w\left((x - \alpha z)^{\mu} S_1, (x - \alpha z)^{\mu} S_2, (x - \alpha z)^{\mu} S_3\right)\\ &\equiv (x - \alpha z)^{\mu(n-1)}\, w\,(S_1, S_2, S_3). \end{aligned}$$

Wegen $B(\alpha z, y, z) \not\equiv 0\,[(y - \beta z)^2]$ wird

$$(x - \alpha z, B) = 1 \text{ und } \left((x - \alpha z)^{\mu(n-1)}, B\right) = \mu(n - 1)$$

bezüglich π. Wir erhalten also aus (24) und (15) die nachstehenden Multiplizitätsrelationen

$$(25)\quad \begin{aligned} &(U, B) = \mu(n-1) + \delta_1;\ (V, B) = \mu(n-1) + \delta_2;\\ &(W, B) = \mu(n-1) + \delta_3, \text{ wenn wir zur Abkürzung setzen:} \end{aligned}$$

$$\delta_1 = \left(u(S_1, S_2, S_3), B\right);\ \delta_2 = \left(v(S_1, S_2, S_3), B\right);\ \delta_3 = \left(w(S_1, S_2, S_3), B\right).$$

Wir behaupten:

(26) Wenigstens eine der drei Zahlen δ_1, δ_2, δ_3 ist Null.

Das Gegenteil nämlich, wenn sämtliche δ größer als Null wären, bedeutete, daß die drei Formen $u(S_1, S_2, S_3)$, $v(S_1, S_2, S_3)$, $w(S_1, S_2, S_3)$ gleichzeitig verschwinden für $x = \alpha z$, $y = \beta z$, daß also — gemäß der Definition der u, v, w — die drei Formen A_x, A_y, A_z die folgende Nullstelle gemeinsam hätten:

$$x = S_1(\alpha, \beta, 1) = p;\ y = S_2(\alpha, \beta, 1) = q;\ z = S_3(\alpha, \beta, 1) = r$$

mit $(p, q, r) \neq (0, 0, 0)$ wegen (22), daß also A selbst, entgegen der Voraussetzung, eine mindestens zweifach zählende Nullstelle hätte, nämlich diese: $x = p$, $y = q$, $z = r$. Somit ist (26) bewiesen.

Nun gehen wir zu den Multiplizitätsrelationen (16) zurück. Über die drei Funktionaldeterminanten, welche in (16) aufgetreten waren, können wir folgendes aussagen: Sie sind teilerfremd zu B wegen (12). Ferner, auf Grund des H. III:

Wenn für eine f, g, h und B gemeinsame Nullstelle π gilt

$$(f, B) \geqq \mu; \quad (g, B) \geqq \mu; \quad (h, B) \geqq \mu,$$

so gilt für dieselbe Nullstelle π:

$$(27) \quad \left(\binom{f, g, B}{x, y, z}, B\right) \geqq 2\mu; \left(\binom{g, h, B}{x, y, z}, B\right) \geqq 2\mu; \left(\binom{h, f, B}{x, y, z}, B\right) \geqq 2\mu.$$

Das gilt auch noch für $\mu = 0$, in trivialer Weise. Auf diese Tatsache (27) stützt sich wesentlich die nachstehende noch zu beweisende Ungleichung[1]

$$(28) \qquad (W, B) \leqq \left(\binom{f, g, B}{x, y, z}, B\right) + \mu(n-3,$$

in der μ die kleinste der drei Zahlen $(f, B), (g, B), (h, B)$ bedeutet.

Wir unterscheiden 3 Fälle, entsprechend dem Satz (26). Sei $\delta_1 = 0$; dann folgt aus $(16)_2$ und $(27)_2$

$$(W, B) \leqq \mu(n-3) + \left(\binom{f, g, B}{x, y, z}, B\right)$$

Das ist aber gerade die Ungleichung (28).

Sei $\delta_2 = 0$; dann folgt aus $(16)_1$ und $(27)_3$

$$\mu(n-3) + \left(\binom{f, g, B}{x, y, z}, B\right) \geqq (W, B),$$

also wiederum (28).

Sei $\delta_3 = 0$; dann folgt schon aus $(27)_1$, nachdem man beiderseits $\mu(n-3)$ addiert hat

$$\left(\binom{f, g, B}{x, y, z}, B\right) + \mu(n-3) \geqq \mu(n-1) = W, B).$$

Somit ist (28) allgemein bewiesen. Die Summation über alle[2] gemeinsamen Nullstellen von W und B ergibt aus (28) sofort

[1] Durch zyklische Vertauschungen gewinnt man analoge Ungleichungen für (U, B) und für (V, B), von denen wir aber keinen Gebrauch machen.

[2] Für die Summe der Multiplizitätszahlen aller gemeinsamen Nullstellen von zwei teilerfremden Formen L und M schreiben wir kurz $[L, M]$. Dieses Symbol bedeutet also eine Zahl, und zwar, nach Bézout, das Produkt der Ordnungszahlen von L und M.

$$(29) \qquad [W, B] \leqq \left[\binom{f, g, B}{x, y, z}, B\right] + (n-3)\,\sigma$$

$$\text{mit } \sigma = \mu_1 + \mu_2 + \ldots + \mu_r.$$

Infolge des Bézoutschen Satzes folgt weiter

$$m(n-1)\,n \leqq (2m + n - 3)\,n + (n-3)\,\sigma$$
$$m(n-3)\,n \leqq (n-3)\,n + (n-3)\,\sigma,$$

und daher, falls $n > 3$ ist,

$$m \cdot n \leqq n + \sigma$$

$$(30) \qquad (m-1)\,n \leqq \sigma.$$

Somit ist Hilfsatz VI bewiesen.

§ 5. Beseitigung gemeinsamer Teiler von zwei der drei Formen f, g, h.

Wie aus der Anmerkung S. 157 hervorgeht, darf man ohne Beschränkung der Allgemeinheit die Form A einer linearen homogenen umkehrbaren Transformation unterwerfen. Dadurch kann man unter anderem erreichen, daß die Potenzen x^n und y^n und z^n je mit von 0 verschiedenen Koeffizienten als Glieder der Form A, welche ja n^{ter} Ordnung ist, vorkommen. Wir wollen eine so zubereitete Form A kurz als „präpariert" bezeichnen. Wir beweisen zunächst:

Wenn für irgendeinen Punkt π gilt:

$$(31) \qquad (f, B) \geqq \mu \text{ und gleichzeitig } (g, B) \geqq \mu,$$

so ist auch stets $(h, B) \geqq \mu$, falls A präpariert ist.

Beweis: Es sei $A = z^n + C_{(x,y,z)}$ mit

$$C = z^0 E_n(x, z) + z^1 \cdot E_{n-1}(x, y) + z^2 E_{n-2}(x, y) + \ldots + z^{n-1} E_1(x, y).$$

Dabei bedeutet E_k eine Binärform k^{ter} Ordnung in x, y. Ist nun $\alpha x + by$ nicht identisch Null, so folgt[1] aus H. IV jedenfalls $(af + bg, B) \geqq \mu$. Also hat jede nicht identisch verschwin-

[1] $af + bg \equiv 0\ [B]$ kann bei einem wesentlich nicht linearen Tripel f, g, h nicht vorkommen. Wegen der Begründung vergleiche man den Beweis der Ungleichung (11).

dende Binärform k^{ter} Ordnung, etwa $E_k(x, y)$, die Eigenschaft $(E_{k(f,g)}, B) \geqq k\mu$. Wegen

$$A(f,g,h) = h^n + C(f,g,h) \equiv o\,[B]$$

mit $h^n \not\equiv o\,[B]$ ist auch $C(f,g,h) \not\equiv o\,[B]$. Wäre nun, entgegen der Behauptung (31) etwa $(h, B) = \nu < \mu$, so ergäbe H. IV, wiederholt angewandt:

$$\big(C(f,g,h), B\big) \geqq \big(h^{n-1} E_1(f,g), B\big) \geqq (n-1)\nu + \mu,$$

also $\big(C(f,g,h), B\big) > n\nu$.

Andererseits ist $(h^n, B) = n\nu$, also nach H. IV $A(f,g,h) = h^n + C(f,g,h) \not\equiv o\,[B]$, entgegen der Voraussetzung.

Somit ist (31) bewiesen.

Mit Hilfe (31) kommt man leicht zu dem Hilfsatz VII:

Wenn A präpariert und wenn f, g, h ein zu A gehöriges Formentripel ist, und wenn die Formen g und h einen gemeinsamen Teiler t besitzen, etwa

$$g = t\psi \text{ und } h = t\chi,$$

so gibt es auch eine Form φ, so daß

$$f \equiv t\varphi \mod B$$

ist. Tripel f, g, h ist also äquivalent, im Sinne des Hauptsatzes, mit φ, ψ, χ, wo ψ und χ — das ist das Wesentliche — teilerfremd sind.

Beweis: Wegen (31) ist nämlich $(f, B) \geqq \mu$ für jede gemeinsame Nullstelle π von t und B, wo μ die kleinste der Zahlen (g, B) und (h, B) ist.

Wegen $(g, B) \geqq (t, B)$ und $(h, B) \geqq (t, B)$ bezüglich π ist also auch $(f, B) \geqq (t, B)$.

Daher gibt es nach H. I eine Form φ, so daß

$$f \equiv t\varphi \mod B$$

ist. Somit ist Hilfsatz VII bewiesen.

§ 6. Reduktion des Grades der Transformation von m auf $\left[\frac{n+1}{2}\right]$.

Zunächst zwei Tatsachen einfacher Art.

(32) Wenn π_1 und π_2 zwei verschiedene Punkte bedeuten, repräsentiert durch $\alpha_1, \beta_1, \gamma_1$ und $\alpha_2, \beta_2, \gamma_2$, so daß also

$$\alpha_1 : \beta_1 : \gamma_2 \neq \alpha_2 : \beta_2 : \gamma_2,$$

so gibt[1] es eine lineare Form $L = ax + by + cz$, welche π_1 und π_2 zu Nullstellen hat.

(33) Zu jeder Form B mit der einfachen Nullstelle π gibt[2] es eine lineare Form $L = ax + by + cz$ von der Art, daß für π gilt: $(L, B) \geqq 2$.

Auf Grund von (32) kann man schon folgende Aufgabe lösen: Eine nicht lineare irreduzible Form B habe die Nullstellen $\pi_1, \pi_2, \ldots, \pi_r$. Gesucht ist eine Form Q, für die $\pi_1, \pi_2, \ldots, \pi_r$ ebenfalls Nullstellen sind, aber so, daß Q teilerfremd zu B und außerdem so ist, daß die Multiplizität (Q, B) für jeden der genannten Punkte einen vorgeschriebenen Mindestwert erreicht, und

---

[1] Die zugehörigen Koeffizienten a, b, c haben, bis auf eine gemeinsame multiplikative Konstante, die Werte

$$a = \beta_1\gamma_2 - \beta_2\gamma_1;\ b = \gamma_1\alpha_2 - \gamma_2\alpha_1;\ c = \alpha_1\beta_2 - \alpha_2\beta_1.$$

[2] Die zugehörigen Koeffizienten a, b, c haben stets, bis auf eine gemeinsame multiplikative Konstante, die Werte

$$a = \frac{\partial B(\alpha,\beta,\gamma)}{\partial x};\ b = \frac{\partial B(\alpha,\beta,\gamma)}{\partial y};\ c = \frac{\partial B(\alpha,\beta,\gamma)}{\partial z}.$$

Man verifiziert diese Tatsache leicht mit einer von mir aufgestellten Regel (vgl. § 2 der Abhandlung H. Kapferer, Über Schnittpunktsysteme mit vorgeschriebenen Multiplizitätszahlen. Heidelberger Akademieberichte, 1930) oder auch dadurch, daß man beachtet, daß L wegen $nB = xB_x + yB_y + zB_z$ auch so angeschrieben werden kann:

$$L = B_x(\alpha, \beta, \gamma)[x - \alpha z] + B_y(\alpha, \beta, \gamma)[y - \beta z],$$

und zeigt, daß, wenn B nach Dimensionen in den Linearformen $(x - \alpha z)$ und $(y - \beta z)$ geordnet wird, etwa

$$B = z^{n-1}B_1 + z^{n-1}B_2 + \ldots + z^0 B_n,$$

das Glied B_1 nichts anderes ist als gerade L, bis auf eine multiplikative Konstante.

zwar soll $(Q, B) \geqq \mu_i$ bezüglich Punkt π_i vorgeschrieben sein; $i = 1, 2, \ldots r$.

Eine Lösung ergibt sich dadurch, daß man die gegebenen Punkte paarweise auf eine genügende Anzahl von linearen Formen ($\left[\frac{1+r}{2}\right]$ solche sind sicher ausreichend) verteilt, gemäß (32), und das Produkt der letzteren bildet, hierauf eine genügend hohe Potenz dieses Produktes mit Q bezeichnet. (Es ist sicher ausreichend, für den Exponenten die größte der Zahlen $\mu_1, \mu_2, \ldots, \mu_r$ zu wählen.) Hierbei ist dann ohne weiteres Q teilerfremd zu B, weil B irreduzibel und nicht linear ist. — Auf Grund von (33) — das ist für das Folgende das Entscheidende — kann man aber ohne weiteres die Ordnung von Q auf $\left[\frac{1+\sigma}{2}\right]$ herabdrücken, wo $\sigma = \mu_1 + \mu_2 + \cdots + \mu_2$ ist.

Nun beweisen wir folgenden Hilfsatz VIII.

Bei $n > 3$ gibt es zu jedem wesentlich nicht linearen Formentripel f, g, h ein ihm äquivalentes Tripel $f, g, \bar{h}$ von der Ordnung $\bar{m} = \left[\frac{n+1}{2}\right]$.

Beweis von H. VIII. Wir wissen aus H. VI, daß bei $n > 3$ die Anzahl σ der gemeinsamen Nullstellen der drei Kurvenpaare

$$f = 0,\ B = 0;\quad g = 0,\ B = 0;\quad h = 0,\ B = 0,$$

jede mit derjenigen Multiplizität gezählt, welche die kleinste der 3 Zahlen (f, B), (g, B), (h, B) angibt, die Eigenschaft hat:

$$\sigma \geqq (m - 1)\, n.$$

Man denke sich nun von diesen σ Nullstellen irgendwelche $(m - 1)n$ ausgewählt, so daß also das Schnittsystem

$$h = 0,\ B = 0$$

aus diesen ausgewählten $(m - 1)$ n-Punkten und noch weiteren n-Punkten besteht, jeweils einschließlich der Multiplizität gezählt. Die letzteren n-Punkte verteilen wir, wie oben, gemäß (32) und (33) auf $\left[\frac{n+1}{2}\right]$ lineare Formen. Das Produkt $\bar{h}$ derselben ist genau von der Ordnung $\left[\frac{n+1}{2}\right]$ und ist teilerfremd

zu B, weil B irreduzibel und nicht linear ist ($n > 3$). Wir definieren nun

$$\bar{h}f = F;\ \bar{h}g = G;\ \bar{h}h = H.$$

Für jede gemeinsame Nullstelle von h und B gilt sicher

$$(F, B) \geqq (h, B) \text{ und } (G, B) \geqq (h, B).$$

Daher gibt es nach H. I (zweimal angewandt) sicher zwei Formen $\bar{f}$ und $\bar{g}$ der Art, daß

$$F \equiv \bar{f}h \bmod B \text{ und gleichzeitig } G \equiv \bar{g}h \bmod B$$

ist. Aus der Kongruenz $A\,(F, G, H) \equiv 0\,[B]$ läßt sich h, wegen $h \not\equiv 0\,[B]$ nach (11), herausdividieren.

In $\bar{f}, \bar{g}, \bar{h}$ haben wir somit ein neues Formentripel gewonnen.

Auf Grund der Definition von $\bar{f}, \bar{g}, \bar{h}$ gelten die Kongruenzen:

$$\lambda f \equiv \mu\bar{f} \text{ und } \lambda g \equiv \mu\bar{g} \text{ und } \lambda h \equiv \mu\bar{h},$$

jeweils mod B, für $\lambda = \bar{h}$ und $\mu = h$.

Also sind f, g, h und $\bar{f}, \bar{g}, \bar{h}$ einander äquivalent in dem oben (S. 1) definierten Sinn, also wegen (34) beide wesentlich nicht linear im Sinne des Hauptsatzes.

Somit ist Hilfsatz VIII bewiesen.

§ 7. Die Ungleichung $n < 4$.

A sei präpariert. $A\,(f, g, h) \equiv 0\,[B]$.

Nach H. VIII dürfen wir annehmen, daß die gemeinsame Ordnung m der Formen f, g, h höchstens gleich $\left[\frac{n+1}{2}\right]$ ist. Nach H. VII dürfen wir weiter annehmen, daß g und h teilerfremd sind. Nach H. VI wissen wir, daß bei $n > 3$ und gleichzeitig $m > 1$ wenigstens eine gemeinsame Nullstelle von f, g, h und B vorhanden sein muß. Auf jede dieser Nullstellen ist H. V anwendbar, nachdem die Teilerfremdheit von g und h feststeht, also

$$(g, h) \geqq \mu,$$

wo μ die kleinste der Zahlen (g, B) und (h, B) ist. Die Summation über alle gemeinsamen Nullstellen von f, g, h und B ergibt

$$[g, h] \geqq \mu_1 + \mu_2 + \cdots + \mu_r = \sigma.$$

Nach H. VI ist andererseits $\sigma \geqq (m-1)\, n$, also

$$\begin{gathered} [g, h] \geqq \sigma \geqq (m-1)\, n \\ m^2 \geqq \sigma \geqq (m-1)\, n \\ m^2-1 \geqq \sigma-1 \geqq (m-1)\, n-1. \end{gathered} \tag{34}$$

Wegen $m > 1$ ergibt die Division durch $(m-1)$

$$m + 1 \geqq n - \frac{1}{m-1}.$$

Hierbei ist also m mindestens 2 und höchstens $\left[\frac{n+1}{2}\right]$.

Sei zunächst $m = 2$; dann folgt

$$3 \geqq n-1, \text{ also } 4 \geqq n.$$

Sei $m > 2$; dann ist sogar

$$\begin{gathered} m + 1 \geqq n \\ \frac{n+3}{2} \geqq n \\ 3 \geqq n. \end{gathered}$$

Es bleibt also nur der Fall $m = 2$ bei $n = 4$ zu behandeln übrig.

Aus (34) folgt zunächst, daß hier σ genau $(m-1)\, n = 4$ ist, welche Möglichkeit in (30) offengelassen war. Dann wird rückwirkend auch (29) übergehen in die genaue Gleichung

$$[W, B] = [I, B] + (n-3)\, \sigma,$$

also insbesondere bei $n = 4$, in

$$[W, B] = [I, B] + 4, \tag{35}$$

wo $I = \begin{pmatrix} f, g, B \\ x, y, z \end{pmatrix}$ gesetzt ist.

Das bedeutet aber, daß I und B überhaupt keine gemeinsame Nullstellen haben außer solchen, die auch W und B gemeinsam sind, daß also

$$(W, B) \geqq (I, B)$$

ist für jede gemeinsame Nullstelle von I und W, daß also nach H. I eine lineare Form t_1 existieren muß, so daß

$$W \equiv t_1 I \bmod B_4,$$

und daß, wegen (35), das Schnittsystem $t_1 = 0$, $B_4 = 0$ gerade erschöpft wird durch die 4 Nullstellen.

Nun sei f_2, g_2, h_2 das im Falle $m = 2$, $n = 4$ vorliegende Tripel. Nach H. I muß es dann 3 lineare Formen f_1, g_1, h_1 geben, so daß die Kongruenzen gelten

$$f_2 \equiv t_1 f_1;\ g_2 \equiv t_1 g_1;\ h_2 \equiv t_1 h_1,$$

jeweils mod B. Also wäre f_2, g_2, h_2 äquivalent einem linearen Tripel. Das widerspricht der Voraussetzung. Somit ist auch der Fall $n = 4$ bei $m = 2$ unmöglich, und die Ungleichung $n < 4$ im Sinne des Hauptsatzes bewiesen.