Sitzungsberichte

der

mathematisch-naturwissenschaftlichen Abteilung

der

Bayerischen Akademie der Wissenschaften

zu München

1928. Heft II
Mai- bis Julisitzung

München 1928
Verlag der Bayerischen Akademie der Wissenschaften
in Kommission des Verlags R. Oldenbourg München

Über den größten gemeinsamen Teiler von zwei Polynomen.

Von **Oskar Perron.**

Vorgelegt in der Sitzung am 5. Mai 1928.

Einleitung.

Sind $f(x)$, $g(x)$ zwei Polynome von den Graden m, n und ist ihr größter gemeinsamer Teiler $d(x)$ vom Grad k, so hängt der Verlauf des Euklidischen Algorithmus nicht nur von m, n, k ab, sondern wesentlich auch von den Koeffizienten der Polynome $f(x)$, $g(x)$. Beispielsweise kann man leicht beliebig viele Polynompaare angeben, bei denen der Algorithmus schon nach dem ersten Schritt abbricht, und ebenso leicht andere, bei denen er länger dauert. Der Euklidische Algorithmus liefert daher kein einheitliches Bildungsgesetz für die Koeffizienten von $d(x)$. Merkwürdigerweise existiert aber trotzdem ein solches Bildungsgesetz. Für diesen Satz, auf dessen Wichtigkeit mich Herr Hasse aufmerksam gemacht hat, hat Heinrich Weber einen nicht ganz leicht zu verstehenden Beweis gegeben[1]). Ich werde nachstehend im § 1 einen einfacheren Beweis des Satzes mitteilen und dann im § 2 zeigen, daß ein analoger Satz für Polynome von mehreren Variabeln nicht gilt.

[1]) Lehrbuch der Algebra; kleine Ausgabe, Braunschweig 1912, S. 105.

§ 1.

Polynome von einer Variabeln.

Der Satz ist folgendermaßen zu formulieren:

Lehrsatz. Seien m, n, k positive ganze Zahlen und zwar $k \leqq m$ und $k \leqq n$. Sind dann

$$a_0, a_1, \ldots, a_m; \; b_0, b_1, \ldots, b_n$$

$m + n + 2$ unabhängige Variable, so gibt es $k + 1$ Polynome dieser Variabeln mit ganzzahligen Koeffizienten

$$H_\varkappa(a_0, a_1, \ldots, a_m; \; b_0, b_1, \ldots, b_n) \qquad (\varkappa = 0, 1, \ldots, k)$$

von folgender Beschaffenheit:

Sobald zwei Polynome $f(x)$, $g(x)$ von den Graden m und n

$$f(x) = a_0' x^m + a_1' x^{m-1} + \cdots + a_m' \qquad (a_0' \neq 0),$$
$$g(x) = b_0' x^n + b_1' x^{n-1} + \cdots + b_n' \qquad (b_0' \neq 0)$$

einen größten gemeinsamen Teiler $d(x)$ vom Grad k haben:

$$d(x) = x^k + c_1 x^{k-1} + \cdots + c_k,$$

ist $H_0(a_0', \ldots, a_m'; \; b_0', \ldots, b_n') \neq 0$, und die Koeffizienten $c_\varkappa$ von $d(x)$ lassen die folgende Darstellung zu:

$$c_\varkappa = \frac{H_\varkappa(a_0', \ldots, a_m'; \; b_0', \ldots, b_n')}{H_0(a_0', \ldots, a_m'; \; b_0', \ldots, b_n')} \qquad (\varkappa = 1, 2, \ldots, k).$$

Beweis. Für $k = m$ ist der Satz evident, indem man einfach $H_\varkappa = a_\varkappa$ setzen kann; ebenso für $k = n$, in welchem Fall man $H_\varkappa = b_\varkappa$ setzen kann. Sei daher $k < m$ und $k < n$. Dann kann man jedenfalls drei Polynome von x

$$\xi_0 x^{n-k-1} + \xi_1 x^{n-k-2} + \cdots + \xi_{n-k-1},$$
$$\eta_0 x^{m-k-1} + \eta_1 x^{m-k-2} + \cdots + \eta_{m-k-1},$$
$$\zeta_0 x^k + \zeta_1 x^{k-1} + \cdots + \zeta_k,$$

die nicht alle drei identisch verschwinden, so bestimmen, daß die folgende Identität besteht:

$$(1) \quad \begin{cases} (a_0 x^m + a_1 x^{m-1} + \cdots + a_m)(\xi_0 x^{n-k-1} + \xi_1 x^{n-k-2} + \cdots + \xi^{n-k-1}) \\ + (b_0 x^n + b_1 x^{n-1} + \cdots + b_n)(\eta_0 x^{m-k-1} + \eta_1 x^{m-k-2} + \cdots + \eta_{m-k-1}) \\ + \zeta_0 x^k + \zeta_1 x^{k-1} + \cdots + \zeta_k = 0. \end{cases}$$

Denn das ergibt für die $m+n-k+1$ unbekannten Koeffizienten ξ_ν, η_μ, $\zeta_\varkappa$ nur $m+n-k$ lineare homogene Bedingungsgleichungen:

$$(2)\quad \begin{cases} a_0\xi_0 & + b_0\eta_0 & = 0, \\ a_1\xi_0 + a_0\xi_1 & + b_1\eta_0 + b_0\eta_1 & = 0, \\ \cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots & \cdots\cdots \\ a_m\xi_{n-k-1} & + b_n\eta_{m-k-1} + \zeta_k & = 0, \end{cases}$$

die also gewiß eine nichttriviale Lösung haben. Wir werden sehen, daß die $(m+n-k)$-reihigen Determinanten der Matrix des Systems (2) nicht alle verschwinden, so daß es nur eine nichttriviale Lösung gibt und wir diese in der Form

$$(3)\quad \begin{cases} \xi_\nu = F_\nu(a_0, a_1, \ldots, a_m;\ b_0, b_1, \ldots, b_n), \\ \eta_\mu = G_\mu(a_0, a_1, \ldots, a_m;\ b_0, b_1, \ldots, b_n), \\ \zeta_\varkappa = H_\varkappa(a_0, a_1, \ldots, a_m;\ b_0, b_1, \ldots, b_n) \end{cases}$$

schreiben können, wo die F_ν, G_μ, $H_\varkappa$ solche Determinanten (vom Vorzeichen abgesehen) sind, also Polynome mit ganzzahligen Koeffizienten.

Zum Beweis spezialisieren wir die Variabeln a_μ, b_ν zu a'_μ, b'_ν und machen den zu (1) analogen Ansatz

$$(1')\quad \begin{cases} (a'_0x^m + a'_1x^{m-1} + \cdots + a'_m)(\xi'_0x^{n-k-1} + \xi'_1x^{n-k-2} + \cdots + \xi'_{n-k-1}) \\ + (b'_0x^n + b'_1x^{n-1} + \cdots + b'_n)(\eta'_0x^{m-k-1} + \eta'_1x^{m-k-2} + \cdots + \eta'_{m-k-1}) \\ + \zeta'_0x_k + \zeta'_1x^{k-1} + \cdots + \zeta'_k = 0, \end{cases}$$

wobei dann analog zu (2) auch

$$(2')\quad \begin{cases} a'_0\xi'_0 & + b'_0\eta'_0 & = 0, \\ a'_1\xi'_0 + a'_0\xi'_1 & + b'_1\eta'_0 + b'_0\eta'_1 & = 0, \\ \cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots & \cdots\cdots \\ a'_m\xi'_{n-k-1} & + b'_n\eta'_{m-k-1} + \zeta_k & = 0 \end{cases}$$

ist. Dabei sollen die ξ'_ν, η'_μ, $\zeta'_\varkappa$ eine beliebige nichttriviale Lösung dieses Gleichungssystems bedeuten. Da nun die beiden Polynome

$$a'_0x^m + a'_1x^{m-1} + \cdots + a'_m,$$
$$b'_0x^n + b'_1x^{n-1} + \cdots + b'_n$$

den größten gemeinsamen Teiler

$$d(x) = x^k + c_1x^{k-1} + \cdots + c_k$$

haben sollen, so folgt aus (1'), daß auch $\zeta'_0x^k + \zeta'_1x^{k-1} + \cdots + \zeta'_k$ durch $d(x)$ teilbar ist. Folglich ist

$$\zeta'_\varkappa = c_\varkappa \zeta'_0 \qquad (\varkappa = 1, 2, \ldots, k), \tag{4}$$

und indem man (1′) durch $d(x)$ dividiert, entsteht eine Identität der Form

$$\begin{aligned} &f_1(x)\cdot(\xi'_0 x^{n-k-1} + \cdots + \xi'_{n-k-1}) \\ &+ g_1(x)\cdot(\eta'_0 x^{m-k-1} + \cdots + \eta'_{m-k-1}) + \zeta'_0 = 0, \end{aligned} \tag{5}$$

wobei $f_1(x)$, $g_1(x)$ zwei relativ prime Polynome von den Graden $m-k$ und $n-k$ sind. Daraus erkennt man, daß $\zeta'_0 \neq 0$ ist; denn andernfalls würden nach (4) alle $\zeta'_\varkappa$ und nach (5), weil $f_1(x)$ und $g_1(x)$ relativ prim sind, auch alle ξ'_ν, η'_μ verschwinden, während doch die ξ'_ν, η'_μ, $\zeta'_\varkappa$ eine nichttriviale Lösung des Systems (2′) sein sollten. Da somit für jede nichttriviale Lösung von (2′) stets $\zeta'_0 \neq 0$ ist, so hat dieses System überhaupt nur eine nichttriviale Lösung. Folglich ist sein Rang gleich $m+n-k$, und speziell die der Unbekannten ζ'_0 zugeordnete $(m+n-k)$-reihige Determinante $H_0(a'_0, \ldots, a'_m; b'_0, \ldots, b'_n)$ ist von Null verschieden. Erst recht muß sie also vor der Spezialisierung der Variabeln a_μ, b_ν von Null verschieden gewesen sein, womit die obige Behauptung bewiesen ist. Nach der Spezialisierung ist aber

$$\frac{\zeta'_\varkappa}{\zeta'_0} = \frac{H_\varkappa(a'_0, \ldots, a'_m; b'_0, \ldots, b'_n)}{H_0(a'_0, \ldots, a'_m; b'_0, \ldots, b'_n)} \qquad (\varkappa = 1, 2, \ldots, k),$$

und mit Rücksicht auf (4) ist damit der Lehrsatz bewiesen.

Indem man für die $H_\varkappa$ die aus dem Gleichungssystem (2′) sich ergebenden $(m+n-k)$-reihigen Determinanten hinschreibt, erhält man für das Polynom

$$\zeta'_0 x^k + \zeta'_1 x^{k-1} + \cdots + \zeta'_k$$

die folgende Darstellung als $(m+n-k+1)$-reihige Determinante:

$$\left|\begin{array}{ccccccccc}
a'_0 & & & b'_0 & & & & & \\
a'_1 & a'_0 & & b'_1 & b'_0 & & & & \\
\vdots & \vdots & & \vdots & \vdots & & & & \\
a'_m & \vdots & a'_0 & b'_n & \vdots & b'_0 & & & \\
 & a'_m & \vdots & \vdots & b'_n & \vdots & & & \\
 & & a'_{m-k} & & b'_{n-k} & 1 & 0 & \cdots & 0 \\
 & & \vdots & & \vdots & 0 & 1 & \cdots & 0 \\
 & & \vdots & & \vdots & \vdots & \vdots & \cdots & \vdots \\
 & & a'_m & & b'_n & 0 & 0 & \cdots & 1 \\
 & & 0 & & 0 & x^k & x^{k-1} & \cdots & 1
\end{array}\right|, \tag{6}$$

wobei $n-k$ Spalten mit a'_μ, dann $m-k$ Spalten mit b'_ν und dann noch $k+1$ weitere Spalten folgen. Die leeren Felder sind mit Nullen zu besetzen.

Diese Determinante gibt also, wenn man sie noch durch den Koeffizienten von x^k dividiert, den größten gemeinsamen Teiler $d(x)$, sobald dieser vom Grad k ist.

§ 2.

Polynome von zwei Variabeln.

Es soll jetzt gezeigt werden, daß bei Polynomen von mehreren Variabeln schon in den einfachsten Fällen ein Analogon zu dem Satz des vorigen Paragraphen nicht existiert. Zu dem Zweck nehmen wir zwölf unabhängige Variabeln

$$a_1, a_2, a_3, a_4, a_5, a_6,$$
$$b_1, b_2, b_3, b_4, b_5, b_6,$$

und nehmen an, es gäbe drei Polynome dieser Variabeln

$$(7)\quad F\begin{pmatrix} a_1, \ldots, a_6 \\ b_1, \ldots, b_6 \end{pmatrix}, \qquad G\begin{pmatrix} a_1, \ldots, a_6 \\ b_1, \ldots, b_6 \end{pmatrix}, \qquad H\begin{pmatrix} a_1, \ldots, a_6 \\ b_1, \ldots, b_6 \end{pmatrix}$$

von folgender Beschaffenheit: Allemal wenn die beiden Polynome zweiten Grades von x und y

$$(8)\quad \begin{cases} f(x,y) = a'_1 x^2 + a'_2 xy + a'_3 y^2 + a'_4 x + a'_5 y + a'_6, \\ g(x,y) = b'_1 x^2 + b'_2 xy + b'_3 y^2 + b'_4 x + b'_5 y + b'_6 \end{cases}$$

einen größten gemeinsamen Teiler vom ersten Grad haben, ist dieser bis auf einen von x, y freien Faktor gleich

$$F\begin{pmatrix} a'_1, \ldots, a'_6 \\ b'_1, \ldots, b'_6 \end{pmatrix} \cdot x + G\begin{pmatrix} a'_1, \ldots, a'_6 \\ b'_1, \ldots, b'_6 \end{pmatrix} \cdot y + H\begin{pmatrix} a'_1, \ldots, a'_6 \\ b'_1, \ldots, b'_6 \end{pmatrix}.$$

Wir werden sehen, daß diese Annahme auf einen Widerspruch führt, daß es also derartige Polynome F, G, H nicht gibt. Selbst wenn wir für $f(x,y)$ und $g(x,y)$ nur reguläre Polynome zulassen, d. h. solche, bei denen

$$a'_1 \neq 0,\ a'_3 \neq 0,\ b'_1 \neq 0,\ b'_3 \neq 0$$

ist, wird sich unsere Annahme als widerspruchsvoll erweisen.

Zum Beweis wählen wir $f(x, y)$ und $g(x, y)$ in folgender Weise

$$(9)\quad \begin{cases} f(x,y) = (ax+by+c)(px+qy+r) \\ \qquad\quad = apx^2 + (aq+bp)xy + \cdots + cr, \\ g(x,y) = (ax+by+c)(p_1x+q_1y+r_1) \\ \qquad\quad = ap_1x^2 + (aq_1+bp_1)xy + \cdots + cr_1, \end{cases}$$

wobei die neun Größen

$$(10)\qquad a, b, c, p, q, r, p_1, q_1, r_1$$

zunächst unabhängige Variable seien. Wir setzen dann

$$(11)\quad H\begin{pmatrix} ap, & aq+bp, & bq, & ar+cp, & br+cq, & cr \\ ap_1, & aq_1+bp_1, & bq_1, & ar_1+cp_1, & br_1+cq_1, & cr_1 \end{pmatrix} = H^*\begin{pmatrix} a, & b, & c \\ p, & q, & r \\ p_1, & q_1, & r_1 \end{pmatrix}$$

und eine entsprechende Bedeutung mögen

$$F^*\begin{pmatrix} a, & b, & c \\ p, & q, & r \\ p_1, & q_1, & r_1 \end{pmatrix}, \qquad G^*\begin{pmatrix} a, & b, & c \\ p, & q, & r \\ p_1, & q_1, & r_1 \end{pmatrix}$$

haben. Die F^*, G^*, H^* sind Polynome der neun Variabeln (10), und da die Polynome $f(x, y)$, $g(x, y)$ einen mit $ax+by+c$ äquivalenten größten gemeinsamen Teiler haben, muß nach unserer Annahme

$$(12)\quad \begin{aligned} &F^*\begin{pmatrix} a, & b, & c \\ p, & q, & r \\ p_1, & q_1, & r_1 \end{pmatrix}\cdot x + G^*\begin{pmatrix} a, & b, & c \\ p, & q, & r \\ p_1, & q_1, & r_1 \end{pmatrix}\cdot y + H^*\begin{pmatrix} a, & b, & c \\ p, & q, & r \\ p_1, & q_1, & r_1 \end{pmatrix} \\ &\qquad = (ax+by+c)\cdot L\begin{pmatrix} a, & b, & c \\ p, & q, & r \\ p_1, & q_1, & r_1 \end{pmatrix} \end{aligned}$$

sein, wobei L eine nicht identisch verschwindende rationale Funktion der neun Variabeln ist, die sich wegen (12) in der dreifachen Gestalt

$$(13)\qquad L = \frac{F^*}{a} = \frac{G^*}{b} = \frac{H^*}{c}$$

darstellen läßt, woraus man sie als Polynom erkennt[1]).

[1]) Nach Satz 31 meines Buches „Algebra", Band 1. Berlin 1927.

Wenn man jetzt die Größen (10) alle mit Ausnahme von a als unabhängige Variable beläßt, dagegen a zu einer von Null verschiedenen Wurzel des Polynoms L spezialisiert, falls es eine solche gibt, so sind die Polynome $f(x, y)$ und $g(x, y)$ noch immer regulär und ihr größter gemeinsamer Teiler ist mit $ax + by + c$ äquivalent; nach unserer Annahme ist er also auch mit dem Ausdruck (12) äquivalent, was aber andererseits doch nicht zutreffen kann, weil bei unserer Spezialisierung $L = 0$ ist. Somit kann L als Polynom von a keine von Null verschiedene Wurzel haben und hat daher die Form

$$L\begin{pmatrix} a, & b, & c \\ p, & q, & r \\ p_1, & q_1, & r_1 \end{pmatrix} = a^z L_1,$$

wo das Polynom L_1 die Variable a nicht mehr enthält. Genau so erkennt man, daß L auch als Polynom von einer der Variabeln b, p, q, p_1, q_1 keine von Null verschiedene Wurzel hat und als Polynom von einer der Variabeln c, r, r_1 überhaupt keine Wurzel haben kann. Somit hat L die Form

$$L\begin{pmatrix} a, & b, & c \\ p, & q, & r \\ p_1, & q_1, & r_1 \end{pmatrix} = C a^z b^\lambda p^\mu q^\nu p_1^{\mu_1} q_1^{\nu_1}, \tag{14}$$

wo C eine von Null verschiedene Konstante ist.

Aus (14) folgt speziell

$$L\begin{pmatrix} a, & b, & c \\ p, & q, & r \\ p, & q, & r \end{pmatrix} = C a^z b^\lambda p^{\mu+\mu_1} q^{\nu+\nu_1}. \tag{15}$$

Nach (13) und (11) ist aber

$$c \cdot L\begin{pmatrix} a, & b, & c \\ p, & q, & r \\ p, & q, & r \end{pmatrix} = H^*\begin{pmatrix} a, & b, & c \\ p, & q, & r \\ p, & q, & r \end{pmatrix}$$

$$= H\begin{pmatrix} ap, & aq + bp, & bq, & ar + cp, & br + cq, & cr \\ ap, & aq + bp, & bq, & ar + cp, & br + cq, & cr \end{pmatrix}.$$

Hier bleibt die rechte Seite unverändert, wenn man a, b, c mit p, q, r vertauscht, also muß auch die linke Seite unverändert bleiben und es ergibt sich die Funktionalgleichung:

$$c \cdot L\begin{pmatrix} a, & b, & c \\ p, & q, & r \\ p, & q, & r \end{pmatrix} = r \cdot L\begin{pmatrix} p, & q, & r \\ a, & b, & c \\ a, & b, & c \end{pmatrix}.$$

Das links stehende Polynom ist also durch r teilbar, was aber nach (15) nicht der Fall ist. Wegen dieses Widerspruchs ist unsere Annahme, daß es drei Polynome F, G, H der oben angegebenen Art gibt, hinfällig. W. z. b. w.