BAYERISCHE AKADEMIE DER WISSENSCHAFTEN
MATHEMATISCH-NATURWISSENSCHAFTLICHE KLASSE

SITZUNGSBERICHTE

JAHRGANG
1966

MÜNCHEN 1967

VERLAG DER BAYERISCHEN AKADEMIE DER WISSENSCHAFTEN
In Kommission bei der C. H. Beck'schen Verlagsbuchhandlung München

Bemerkungen zur elementaren Algebra: I. Restklassenring und Resultante

Von **Hermann Schmidt** in Würzburg

Vorgelegt am 4. November 1966

Vorbemerkung: Eine Übersicht über die folgenden Betrachtungen enthält das ausführliche Summar zu Beginn dieses Bandes.

1. Gegeben sei ein kommutativer Ring R mit Einselement; $R[x]$ sei der Polynombereich einer Unbestimmten über R. Die Teilbarkeitslehre in diesem stößt auf Schwierigkeiten, falls R Nullteiler enthält, so daß der Satz von der Addition der Grade bei Multiplikation zweier Polynome nicht mehr zu gelten braucht; so ist etwa $(\bar{2}x + \bar{3})\ (\bar{3}x + \bar{2}) = x$ über dem Restklassenring $\{\bar{\nu} | \nu = 0, 1, \ldots 5\}$ der ganzen Zahlen mod 6. Geht man jedoch von einem Polynom $f(x)$ mit höchstem Koeffizienten 1 aus:

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n,$$

so bleibt für Produkte mit einem Faktor $f(x)$ der Gradsatz erhalten, und im Restklassenring $S = R[x]/_{f(x)}$ hat, wie im Falle eines Integritätsbereichs, jede Klasse genau einen Vertreter, der ein Polynom $g(x)$ höchstens $(n-1)$-ten Grades ist. Wir wollen zunächst den Vertreter $\varphi_\nu(x)$ für die Potenz x^ν bestimmen $(\nu = 0, 1, 2 \ldots)$.

Aus $x^\nu f(x) \equiv 0\,(f)$ folgt sofort die Rekursionsformel

$$\varphi_{\nu+n}(x) + a_1 \varphi_{\nu+n-1}(x) + \cdots + a_n \varphi_\nu(x) = 0.$$

Wenn also $\varphi_\nu(x) = \sum_{\mu=0}^{n-1} c_{\nu,\mu} x^\nu$ gesetzt wird, ist bei festem μ $c_{\nu,\mu}$ jene Lösung der Differenzengleichung

$$c_{\nu+n} + a_1 c_{\nu+n-1} + \cdots + a_n c_\nu = 0 \qquad (\nu = 0, 1, 2 \ldots), \tag{1}$$

die der Anfangsbedingung

$$(1)' \qquad c_{\nu,\mu} = \delta_{\nu\mu}$$

(Kroneckersymbol) für $0 \leq \nu \leq n-1$ entspricht. Man erhält also die n-spaltige unendliche Matrix $U = (c_{\nu,\mu})$ durch fortgesetzte Anwendung von (1) auf die Zeilen des Schemas

$$(2) \qquad \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & 1 \\ -a_n & -a_{n-1} & \cdots & -a_1 \\ \cdot & \cdot & \cdots & \cdot \end{pmatrix}.$$

Für ein herausgegriffenes $\mu \leq n-1$ und $\nu \geq \mu$ kommt (1) (1)' ersichtlich auf die folgende Gleichheit im Ring $R\langle t\rangle$ der formalen, gewöhnlichen Potenzreihen über R hinaus:

$$1 + a_1 t + \cdots + a_{n-\mu-1} t^{n-\mu-1} = (1 + a_1 t + \cdots + a_n t^n)\,(c_{\mu,\mu} + c_{\mu+1,\mu} t + c_{\mu+2,\mu} t^2 + \cdots).$$

Nun kann die formale Reihe für $(1 + a_1 t + \cdots + a_n t^n)^{-1} \in R\langle t\rangle$ durch formales Einsetzen in die geometrische Reihe für $(1-u)^{-1}$ gewonnen werden; das folgt daraus, daß die Abbildung $u \to \sum_{\nu=1}^{\infty} \gamma_\nu t^\nu$ $(\gamma_\nu \in R)$ einen Ringhomomorphismus von $R\langle u\rangle$ in $R\langle t\rangle$ bewirkt.[1] Daher hat man in $R\langle t\rangle$, wenn noch $a_0 = 1$ gesetzt wird,

$$(3) \qquad \sum_{\varkappa=0}^{\infty} c_{\mu+\varkappa,\mu} t^\varkappa = \sum_{\varrho=0}^{n-\mu-1} a_\varrho t^\varrho \sum_{m=0}^{\infty} \left(\sum_{(\lambda_j)} (-1)^{\lambda_1+\cdots+\lambda_n} \frac{(\lambda_1+\cdots+\lambda_n)!}{\lambda_1!\cdots\lambda_n!} \cdot a_1^{\lambda_1} \cdots a_n^{\lambda_n} \right) t^m,$$

[1] Das folgt z. B. aus Bourbaki, Elements de mathématique, Livre II, Algèbre Ch. IV, § 5, No. 5 (1950), ist aber auch direkt leicht nachzurechnen. Bei diesem Verfahren würden sich in der Herleitung der Waringschen Formel bei Perron Algebra I, 3. Aufl. (1951) S. 152/54 Restglieder einsparen lassen.

worin jeweils bei festem m über alle Systeme von n nichtnegativen ganzen Zahlen (λ_j) mit $\sum j\lambda_j = m$ zu summieren ist. Wegen (1)′ genügt es, die Koeffizienten von $t^\varkappa$ für $\varkappa \geq n-\mu$ zu vergleichen; abgesehen von dem für $\varrho = 0$, $m = \varkappa$ hervorgehenden Beitrag ergibt sich hierfür noch eine Summe, die sich nach einfacher Umbezeichnung $\lambda_\varrho + 1 \,|\, \lambda_\varrho$ schreiben läßt:

$$-\sum_{(\lambda_j)} \left\{ \left(\sum (-1)^{\Sigma\lambda_j} \frac{(\Sigma\lambda_j - 1)!}{\Pi(\lambda_j!)} \sum_{\varrho=1}^{n-\mu-1} \lambda_\varrho \right) \cdot \Pi a_j^{\lambda_j} \right\}.$$

Hier läuft jeweils j von 1 bis n, und die äußere Summe ist über alle Systeme mit $\lambda_j \geq 0$, $\sum j\lambda_j = \varkappa$ zu erstrecken. Die Faktoren der Potenzprodukte sind aus dem Bereich Γ der ganzen Zahlen; die Multiplikation ist „äußere" Multiplikation in dem in R enthaltenen, von jenen erzeugten Γ-Modul, was für Char. $R \neq 0$ von Bedeutung ist. Zusammengenommen erhält man schließlich die *Endformel*

$$(4) \qquad c_{\nu,\mu} = \sum \left\{ (-1)^{\Sigma\lambda_j} \frac{(\Sigma\lambda_j - 1)!}{\Pi(\lambda_j!)} (\lambda_{n-\mu} + \cdots + \lambda_n) \cdot \Pi a_j^{\lambda_j} \right\},$$

worin jetzt das Gewicht jedes Glieds $\sum j\lambda_j = \nu - \mu$ ist, und das Ergebnis für alle $\nu > \mu$ richtig ist; die Summe wird für $\nu < n$ null.

2. Faßt man nunmehr den Ring S als (kommutative) Algebra vom Range n über R auf, und wählt man die Klassen $e_\nu = \bar{x}^\nu (\nu = 0, 1, 2, \ldots n-1)$ als Basis ($\bar{x}$ die Klasse von x mod f) so ist in der durch

$$(5) \qquad e_\varkappa e_\lambda = \sum_{\mu=0}^{n-1} c_{\varkappa\lambda,\mu} e_\mu$$

erklärten Multiplikationstafel offenbar $c_{\varkappa\lambda,\mu} = c_{\varkappa+\lambda,\mu}$ in der Bezeichnung von 1. Dabei werden nur die Werte $\nu \leq 2n-2$ benötigt. Man erhält nun bekanntlich die sogenannte reguläre Darstellung[2] von S (bezüglich der Basis $(e_\varkappa)$), indem man jeder Restklasse $g(\bar{x}) = \sum_{\lambda=0}^{n-1} b_\lambda \bar{x}^\lambda$ die durch Bildung der Produkte

[2] Vgl. z. B. Deuring, Algebren, Ergeb. der Math. IV (1934) S. 3 oben.

$x^{\varkappa} g(\bar{x})$ $(0 \leq \varkappa \leq n-1)$ nach (5) Zeile für Zeile hervorgehende Matrix

$$G = \left(\sum_{\lambda=0}^{n-1} b_\lambda c_{\lambda+\varkappa,\mu} \right)_{0 \leq \varkappa,\mu \leq n-1} \tag{6}$$

zuordnet.

Da diese Zuordnung ein Homomorphismus ist, gilt auch

$$G = \sum_{\lambda=0}^{n-1} b_\lambda A^\lambda, \quad \text{wenn } A = \begin{pmatrix} 0 & 1 & \cdot\,\cdot & 0 \\ 0 & 0 & \cdot\,\cdot & 0 \\ \cdot & \cdot & \cdot\,\cdot & \cdot \\ 0 & 0 & \cdot\,\cdot & 1 \\ -a_n, & -a_{n-1}, & \cdot\,\cdot & -a_1 \end{pmatrix} \tag{7}$$

die der Klasse $\bar{x}$ nach (6) (vgl. auch (2)) zugeordnete Matrix bedeutet. Insbesondere ist also $A^\lambda = (c_{\lambda+\varkappa,\mu})$. Die Determinante von G heißt die Norm des Elements (bezüglich der regulären Darstellung). Wir wollen zeigen, daß sie mit der *Resultante* $R(f, g)$ *übereinstimmt* $(g(x) \not\equiv 0)$.

Zum Beweis betrachten wir die $(2n-1)$-reihige quadratische Matrix der Determinante 1:

$$C = \begin{pmatrix} E_n & 0 \\ C_{n-1} & E_{n-1} \end{pmatrix},$$

wo E_n, E_{n-1} Einheitsmatrizen der angegebenen Ordnung sind, während

$$C_{n-1} = \begin{pmatrix} c_{n,\mu} \\ c_{n+1,\mu} \\ \cdot \\ \cdot \\ \cdot \\ c_{2n-2,\mu} \end{pmatrix}_{0 \leq \mu \leq n-1}$$

aus den Zeilen der Nummern $n+1, n+2, \cdots 2n-1$ der Matrix U (vgl. 1. (2)) besteht.

Ferner sei Q die Matrix

$$Q = \begin{pmatrix} b_0 & b_1 & \cdots & b_{n-1} & 0 & \cdots & \\ 0 & b_0 & \cdots & & b_{n-1} & \cdots & \\ & & \cdots & & & & \\ 0 & 0 & \cdots & b_0 & \cdots & & b_{n-1} \\ a_n & \cdot & a_2 & a_1 & 1 & & 0 \\ & \cdot & & \cdots & \cdot & & \\ 0 & & \cdot a_n & a_{n-1} & a_{n-2} & \cdots & 1 \end{pmatrix};$$

diese kann offenbar durch geeignete Zeilen- und Spaltenvertauschungen in die Matrix der Sylvesterschen Determinante übergeführt werden, ihre Determinante ist also bis aufs Vorzeichen die Resultante. Da aber das aus der Hauptdiagonale entspringende Glied übereinstimmt, gilt $\det Q = R(f, g)$. Auf Grund von (1) (1)′ und (6) ergibt sich nun leicht

$$QC = \begin{pmatrix} G & L \\ 0 & F_{n-1} \end{pmatrix}, \tag{8}$$

wo es auf die Elemente der Matrix L vom Typ $(n, n-1)$ nicht ankommt, während $\det F_{n-1} = 1$ ist; und daher ist

$$\det Q = \det G = R(f, g), \tag{9}$$

wie behauptet[3].

3. Es sei nunmehr $R = K$ ein beliebiger *Körper*. Dann läßt sich (9) aus Perron a.a.O.[1] S. 262/263, insbesondere (15) für $y = 0$, gewinnen. Ferner ist G in der zu S isomorphen Matrixalgebra $K[A]$ genau dann Nullteiler, wenn $\det G = 0$. Die Existenz von Nullteilern kommt aber, wenn man S zugrunde legt, darauf hinaus, daß $f(x)$ über K zerlegbar ist (da sonst S ein Körper wäre). Letztere Annahme aber ist damit gleichwertig, daß $f(x)$ mit einem Polynom geringeren Grades $g(x)$ einen Teiler gemein hat, oder also, daß für ein solches die Resultante $R(f, g)$ verschwindet. Nach 2. (7) (9) haben wir also einen doppelten Zugang zu der

[3] Hier wurde, auch falls Grad $g(x) < n-1$ sein sollte, die Resultante für den formalen Grad $n-1$ angesetzt; man sieht aber sofort, daß diese sich, wenn etwa $b_m \neq 0$, $b_{m+1} = b_{m+2} = \cdots = b_{n-1} = 0$ genau auf die dem Grade m entsprechende Resultante reduziert.

Zerlegbarkeitsbedingung

Das Polynom $f(x)$ (vom Grade ≥ 2) über dem Körper K ist daselbst genau dann zerlegbar, wenn die Form

$$F(t_0, t_1, \ldots t_{n-1}) = \det(t_0 E + t_1 A + t_2 A^2 + \cdots + t_{n-1} A^{n-1})$$
$$= R(f(x), t_0 + t_1 x + \cdots + t_{n-1} x^{n-1})$$

der Unbestimmten t_ν in K eine Nullform ist, d. h. für mindestens ein System von Spezialwerten $(t_\nu) = (b_\nu)$ $(\neq (0))$ aus K verschwindet.

(Es wird in letzterem Falle von selbst Grad $g(x) \neq 0$, da ja $\det E = 1$). Da wenn $f(x)$ zerlegbar ist, sicher auch ein Faktor vom Grade $\leq \frac{n}{2}$ existiert, genügt es natürlich, $F(t_0, t_1, \ldots t_m, 0, \ldots 0)$ für $m = \left[\frac{n}{2}\right]$ zu prüfen. Die Zerlegbarkeitsfrage wird hiermit auf *eine* diophantische Bedingung zurückgeführt, die, wenn auch im Einzelfalle gewiß nicht immer bequem zu handhaben, vielleicht bei solchen Körpern von Interesse sein dürfte, bei denen nicht, wie beim rationalen Zahlkörper, über Zerlegbarkeit oder Unzerlegbarkeit mittels endlich vieler Proben entschieden werden kann.