COMPOSITIO MATHEMATICA

KLAUS LANGMANN

Der 4-Werte-Satz in der Zahlentheorie

Compositio Mathematica, tome 82, nº 2 (1992), p. 137-142

<http://www.numdam.org/item?id=CM_1992__82_2_137_0>

Compositio Mathematica **82**: 137–142, 1992.

Der 4-Werte-Satz in der Zahlentheorie

KLAUS LANGMANN

Mathematisches Institut, Universität Münster, Einsteinstraße 62, D-4400 Münster, Germany

Received 22 February 1990; accepted 27 August 1991

In der Theorie der auf ganz $\mathbb{C}$ meromorphen Funktionen wird ein sogenannter "4-Werte-Satz" bewiesen ([4], vgl. auch [2]). Dieser Satz besagt, daß zwei auf $\mathbb{C}$ meromorphe nichtkonstante Funktionen f, g schon gleich sind, wenn für 4 verschiedene Werte $a_1, \ldots, a_4 \in \mathbb{C}$ die Divisorengleichheit $\mathscr{D}(f - a_i) = \mathscr{D}(g - a_i)$ für $1 \leqslant i \leqslant 4$ gilt. Wir beweisen jetzt (Folgerung 2) ein schwächeres zahlentheoretisches Analogon, welches ebenfalls für 3 Werte a_1, a_2, a_3 im allgemeinen falsch wird (s. Gegenbeispiel 3). Als Anwendung von Satz 1 wird in Satz 4 gezeigt, daß die Einschränkung von drei Einsetzungshomomorphismen $\varphi: \mathbb{Z}[X] \to \mathbb{Z}^3$ auf die Teilklasse der Minimalpolynome eines Zahlkörpers L nahezu injektiv ist.

An dieser Stelle sei dem Referenten für wertvolle Anregungen gedankt.

Im folgenden sei L ein fester Zahlkörper (d.h. $[L:\mathbb{Q}] < \infty$) und S eine feste endliche Menge von Bewertungen von L (wobei S alle archimedischen Bewertungen enthalten soll). Für $f \in L^*$ schreiben wir $\mathscr{D}_S(f)$ für den Divisor $\Sigma_{\mathfrak{p} \notin S} \operatorname{ord}_{\mathfrak{p}}(f)\mathfrak{p}$. Bezeichnet $\mathcal{O}_S$ die S-ganzen Zahlen von L, so bedeutet $\mathscr{D}_S(f) = \mathscr{D}_S(g)$, daß für die $\mathcal{O}_S$-Hauptideale eine Gleichheit $f\mathcal{O}_S = g\mathcal{O}_S$ gilt, oder äquivalent ausgedrückt, daß f/g eine S-Einheit ist. Dann gilt:

SATZ 1. *Seien a_1, a_2, a_3 drei verschiedene feste Zahlen aus L, die nicht eine arithmetische Progression bilden* (d.h. $a_i \neq \frac{1}{2}(a_j + a_h)$ *für* $\{i, j, h\} = \{1, 2, 3\}$). *Dann gibt es nur endlich viele Paare $(f, g) \in L^2$ mit $f \neq g$ und*

$$\mathscr{D}_S(f - a_i) = \mathscr{D}_S(g - a_i) \quad \textit{für } 1 \leqslant i \leqslant 3.$$

Bevor wir diesen Satz 1 beweisen, seien noch zwei Bemerkungen gegeben:

FOLGERUNG 2. Seien $a_1, \ldots, a_4$ vier verschiedene feste Zahlen aus L. Dann gibt es nur endlich viele Paare $(f, g) \in L^2$ mit $f \neq g$ und

$$\mathscr{D}_S(f - a_i) = \mathscr{D}_S(g - a_i) \quad \text{für } 1 \leqslant i \leqslant 4.$$

Beweis. Wie können wegen Satz 1 annehmen, daß a_1, a_2, a_3 eine arithmetische Progression bilden. Nach geeigneter Translation und Multiplikation kann oBdA $a_1 = -1$, $a_2 = 0$, $a_3 = 1$ angenommen werden. Wenn dann $a_4 = \frac{1}{2}$ oder $a_4 = 2$ ist, ist a_1, a_2, a_4 keine arithmetische Progression; in allen anderen Fällen ist a_2, a_3, a_4 keine arithmetische Progression. Die Behauptung folgt dann aus Satz 1.

BEMERKUNG 3. Satz 1 ist falsch, wenn a_1, a_2, a_3 eine arithmetische Progression bilden: Wenn $\{a_1, a_2, a_3\} = \{-1, 0, 1\}$ ist und $f := e$, $g := e^{-1}$ oder $f := (1-e)(1+e)^{-1}$, $g := (e-1)(e+1)^{-1}$ für irgendeine S-Einheit e ist, so gilt $\mathscr{D}_S(f - a_i) = \mathscr{D}_S(g - a_i)$ für $1 \leqslant i \leqslant 3$.

Umgekehrt zeigt unser Beweis von Satz 1, daß mit Ausnahme der Paare (f, g) aus Bemerkung 3 unser Satz 1 auch im Falle einer arithmetischen Progression $\{a_1, a_2, a_3\} = \{-1, 0, 1\}$ richtig bleibt:

BEWEIS SATZ 1. Sei $R := \mathscr{O}_S$. Indem eventuell S vergrößert wird, kann oBdA $a_1, a_2, a_3 \in R$ angenommen werden. Es gibt also $e_i \in R^*$ mit $(f - a_i)e_i = (g - a_i)$ für $1 \leqslant i \leqslant 3$. Sei dann

$$\mathscr{F} = \{f \in L;\ \exists g \in L,\ g \neq f \quad \text{und} \quad \exists e_i \in R^* \\ \text{mit } (f - a_i)e_i = (g - a_i) \quad \text{für } 1 \leqslant i \leqslant 3\}.$$

Jedem $f \in \mathscr{F}$ ordnen wir dann irgendein festes Tupel (e_1, e_2, e_3, g) mit obiger Eigenschaft zu. Für $f \in \mathscr{F}$ ergibt sich sofort $e_i \neq e_j$ für $i \neq j$. Weiter folgt

$$f = \frac{a_j - a_i + a_i e_i - a_j e_j}{e_i - e_j}. \tag{I}$$

Angenommen, es würde ein e_j für $1 \leqslant j \leqslant 3$ nur endlich viele Werte annehmen, wenn f innerhalb einer unendlichen Familie $\mathscr{F}_0 \subset \mathscr{F}$ läuft. Indem wir zu einer geeigneten unendlichen Teilfolge $\mathscr{F}_1 \subset \mathscr{F}_0$ übergehen, können wir annehmen, daß dann oBdA $e_1 = \alpha$ für eine feste Zahl α und für alle $f \in \mathscr{F}_1$ wäre.

Weiter können wir, indem wir f durch $f - a_1$ und g durch $g - a_1$ ersetzen, oBdA $a_1 = 0$ annehmen. Aus (I) folgt

$$\frac{-a_2 + a_2 e_2}{e_2 - \alpha} = \frac{-a_3 + a_3 e_3}{e_3 - \alpha}$$

und daraus

$$(a_3 - a_2)e_2 e_3 + (a_2 - a_3\alpha)e_3 + (a_2\alpha - a_3)e_2 = \alpha(a_2 - a_3). \tag{II}$$

Weiter folgt aus (I), daß e_2 und e_3 unendlich viele Werte annehmen müssen, wenn $f \in \mathscr{F}_1$ läuft.

Jetzt benutzen wir den Satz von Evertse, Laurent, van der Poorten und Schlickewei ([1, 3, 5]; im folgenden der Kürze halber nach dem alphabetisch erstgenannten Autor bezeichnet): Ist $M \subset (R^*)^n$ eine feste Teilmenge mit $\Sigma_{i=1}^n \beta_i e_i = \beta$ für festes $\beta \in L^*$, feste $\beta_1, \ldots, \beta_n \in L$ und für alle $(e_1, \ldots, e_n) \in M$ und ist $J \subset \{1, \ldots, n\}$ eine maximale Indexmenge, für die

$$N_J := \left\{(e_1, \ldots, e_n) \in M, \sum_{i \in J} \beta_i e_i = 0\right\}$$

eine unendliche Menge ist, so gibt es zu jedem $j \notin J$ nur endlich viele e_j mit $(e_1, \ldots, e_j, \ldots, e_n) \in N_J$ (indem wir S gegebenenfalls vergrößern, können wir annehmen, daß alle β, $\beta_1, \ldots, \beta_n$ in $R^* \cup \{0\}$ liegen, so daß im Fall $\beta_i \neq 0$ also $\tilde{e}_i := \beta_i e_i$ eine S-Einheit ist). Im folgenden wollen wir wiederholt solche Indexmengen J betrachten und stets kurz "maximale Indexmenge" nennen; die zu N_J gehörende Gleichung $\Sigma_{i \in J} \beta_i e_i = 0$ schreiben wir einfacher als $\Sigma_{i \in J} \tilde{e}_i = 0$.

Ist in (II) $a_2 - a_3\alpha = 0$ oder $a_2\alpha - a_3 = 0$ (beide Ausdrücke können nicht 0 sein, da sonst $a_2 = -a_3$ wäre, also $a_1 = \frac{1}{2}(a_2 + a_3)$ folgte), so kann es wegen $\alpha(a_2 - a_3) \neq 0$ keine weiteren maximalen Indexmengen geben; also folgte nach Evertse, daß e_2 und e_3 nur endlich viele Werte für unendlich viele $f \in \mathscr{F}_1$ annehmen würde, was nicht geht. Ist $(a_2 - a_3\alpha)(a_2\alpha - a_3) \neq 0$, so folgt, daß in (II) entweder keine maximalen Indexmengen auftauchen können (dann sind wir wie eben fertig) oder daß diese maximalen Indexmengen in (II) folgende Gestalt haben:

$$0 = \sum_{i \in J} \tilde{e}_i = (a_2 - a_3\alpha)e_3 + (a_2\alpha - a_3)e_2$$

(die anderen maximalen Indexmengen führen sofort auf den Fall e_2 = konstant oder e_3 = konstant). Mit (II) ist jetzt $(a_3 - a_2)e_2e_3 = \alpha(a_2 - a_3)$; aus diesen beiden Gleichungen ergibt sich eine Gleichung für e_2. Damit nähme wieder e_2 nur endlich viele Werte für unendlich viele $f \in \mathscr{F}_1$ an. Insgesamt haben wir bewiesen, daß alle e_1, e_2, e_3 unendlich viele Werte annehmen, wenn f irgendeine unendliche Teilfolge $\mathscr{F}_0 \subset \mathscr{F}$ durchläuft.

Analog (II) folgt aus (I) die Identität

$$\begin{aligned}(a_2)e_3e_1^{-1} + (-a_3)e_2e_1^{-1} + (a_3 - a_2)e_3e_2e_1^{-1}\\ +(a_2)e_2 + (-a_3)e_3 = (a_2 - a_3).\end{aligned} \tag{III}$$

Jetzt betrachten wir maximale Indexmengen J der Gleichung (III).

Fall 1. $(a_2)e_3e_1^{-1}$ und $(-a_3)e_2e_1^{-1}$ tauchen beide nicht in $\Sigma_{i \in J} \tilde{e}_i = 0$ auf.

Dann nimmt also nach Evertse $e_3e_1^{-1}$ und $e_2e_1^{-1}$ nur endlich viele Werte an, wenn f in einer gewissen unendlichen Teilfolge $\mathscr{F}_0 \subset \mathscr{F}$ läuft. Durch Übergang zu einer unendlichen Teilfolge $\mathscr{F}_1 \subset \mathscr{F}_0$ können wir annehmen, daß es feste Zahlen α, β gibt mit $e_3 e_1^{-1} = \alpha$ und $e_2 e_1^{-1} = \beta$ für alle $f \in \mathscr{F}_1$. Aus $(f - a_i)e_i = (fe_1 - a_i)$ für $i = 2, 3$ folgt dann, wenn diese Gleichung für $i = 2$ mit a_3 und für $i = 3$ mit a_2 multipliziert und dann subtrahiert wird, eine Gleichung

$$f(a_3\beta - a_2\alpha - a_3 + a_2) = a_3 a_2(\beta - \alpha)$$

für unendlich viele f. Deshalb müssen beide Seiten gleich 0 sein. Es folgt $\beta = \alpha = 1$, im Widerspruch zu $e_i \neq e_j$ für $i \neq j$.

Fall 2. $(a_2)e_3e_1^{-1}$ und $(-a_3)e_2e_1^{-1}$ tauchen beide in $\Sigma_{i \in J} \tilde{e}_i = 0$ auf.

Es müssen auch die Summanden $(a_2)e_2$ und $(-a_3)e_3$ in $\Sigma_{i\in J} \tilde{e}_i$ auftauchen, da andernfalls nach Evertse für unendlich viele $f \in \mathscr{F}_0$ dann e_2 oder e_3 nur endlich viele Werte annehmen würde. Deshalb kann $\Sigma_{i\in J} \tilde{e}_i = 0$ nur folgende Form haben:

$$(a_2)e_3e_1^{-1} + (-a_3)e_2e_1^{-1} + (a_2)e_2 + (-a_3)e_3 = 0.$$

Es folgt

$$(a_2)e_1^{-1} + (-a_3)e_2e_1^{-1}e_3^{-1} + (a_2)e_2e_3^{-1} = a_3. \tag{IV}$$

Da für $f \in \mathscr{F}_0$ ja e_1^{-1} unendlich viele Werte durchläuft, folgt nach dem Satz von Evertse, daß die maximalen Indexmengen $\tilde{J}$ von (IV) folgende Gestalt haben müssen:

Fall 2(a). $(a_2)e_1^{-1} + (a_2)e_2e_3^{-1} = 0$.

Fall 2(b). $(a_2)e_1^{-1} + (-a_3)e_2e_1^{-1}e_3^{-1} = 0$.

Fall 2(a) führt mit (IV) zu $e_1^2 = 1$ und damit zum Widerspruch.

Fall 2(b) führt mit (IV) zu $e_3^2 = e_2^2$. Da $e_3 \neq e_2$ sein muß, folgt $e_3 = -e_2$, und wegen Fall 2(b) dann $a_2 = -a_3$, was $a_1 \neq \frac{1}{2}(a_2 + a_3)$ widerspricht.

Fall 3. Bei (III) taucht genau einer der beiden Ausdrücke $(a_2)e_3e_1^{-1}$ und $(-a_3)e_2e_1^{-1}$ in $\Sigma_{i\in J} \tilde{e}_i = 0$ auf.

OBdA sei der auftauchende Summand gleich $(a_2)e_3e_1^{-1}$. Dann muß auch der Summand $(a_3 - a_2)e_3e_2e_1^{-1}$ der Gleichung (III) in $\Sigma_{i\in J} \tilde{e}_i$ auftauchen (da andernfalls nach Evertse sowohl $(-a_3)e_2e_1^{-1}$ als auch $(a_3 - a_2)e_3e_2e_1^{-1}$ nur endlich viele Werte für unendlich viele $f \in \mathscr{F}$ annehmen würde; dann nähme aber auch e_3 nur endlich viele Werte an). Da ja (vgl. Fall 2)) sowieso a_2e_2 und $(-a_3)e_3$ in $\Sigma_{i\in J} \tilde{e}_i$ auftauchen, sieht diese Teilsumme $\Sigma_{i\in J} \tilde{e}_i$ so aus:

$$(a_2)e_3e_1^{-1} + (a_3 - a_2)e_3e_2e_1^{-1} + (a_2)e_2 + (-a_3)e_3 = 0.$$

Es folgt

$$(a_2)e_3e_2^{-1}e_1^{-1} + (a_3 - a_2)e_3e_1^{-1} + (-a_3)e_3e_2^{-1} = -a_2. \tag{V}$$

Jetzt betrachten wir maximale Indexmengen $\tilde{J}$ von (V):

Fall 3(a). $\tilde{J}$ ist leer. Dann nähme $e_3e_2^{-1}e_1^{-1}$ und $e_3e_1^{-1}$ endlich viele Werte an, also auch e_2 nur endlich viele Werte.

Fall 3(b). $(a_2)e_3e_2^{-1}e_1^{-1} + (a_3 - a_2)e_3e_1^{-1} = 0$. In diesem Fall nähme e_2 nur einen Wert an.

Fall 3(c). $(a_2)e_3e_2^{-1}e_1^{-1} + (-a_3)e_3e_2^{-1} = 0$. Hier folgte sofort, daß e_1 nur einen Wert annehmen würde.

Fall 3(d). $(a_3 - a_2)e_3e_1^{-1} + (-a_3)e_3e_2^{-1} = 0$.

Es folgt $e_2(a_3 - a_2) = a_3e_1$. Im Fall 3 gilt aber stets $(-a_3)e_2e_1^{-1} = (a_2 - a_3)$. Aus beiden Gleichungen ergibt sich $e_1^2 = e_2^2$, also $e_1 = -e_2$. Dann führt Fall 3(d) auf $a_3 - a_2 = -a_3$, also wegen $a_1 = 0$ auf $a_3 = \frac{1}{2}(a_1 + a_2)$. Damit ist Satz 1 endgültig bewiesen.

Als Anwendung von Satz 1 sei folgende Aussage über den Einsetzungshomomorphismus gegeben (dabei bezeichne $N(\lambda)$ das absolute Glied des Minimalpolynoms zu λ über K):

SATZ 4. *Seien $L \supset K$ Zahlkörper und $R_L \supset R_K$ endlich erzeugte $\mathbb{Z}$-Algebren mit $Q(R_K) = K$ und $Q(R_L) = L$. Weiter seien a_1, a_2, a_3 drei verschiedene feste Elemente aus R_K, die nicht eine arithmetische Progression bilden. Betrachte*

$$\mathscr{M} = \{P \in R_K[X];\ P \text{ ist Minimalpolynom eines Elementes aus } R_L\}.$$

Dann gilt für fast alle Tupel $(b_1, b_2, b_3) \in (R_K)^3$

$$|\{P \in \mathscr{M};\ P(a_i) = b_i \text{ für } 1 \leqslant i \leqslant 3\}| \leqslant \prod_{i=1}^{3} |\{\lambda R_L \subset R_L;\ N(\lambda) = b_i\}|$$

(wobei $|\ |$ die Mächtigkeit bedeutet).

Beweis. Definiere $k_i := |\{\lambda R_L; N(\lambda) = b_i\}|$. Sei dann $b = (b_1, b_2, b_3)$ so, daß eine aus mehr als $\Pi_{i=k}^3 k_i$ Elementen bestehende Unterklasse $\mathscr{M}(b) \subset \mathscr{M}$ existiert mit $P(a_i) = b_i$ für alle $P \in \mathscr{M}(b)$. Sei dann $\mathscr{N}_1 \equiv \mathscr{N}_1(b)$ die Menge der $f \in R_L$ mit $P(f) = 0$ für ein $P \in \mathscr{M}(b)$. Es ist $|\mathscr{N}_1| > \Pi_{i=1}^3 k_i$. Weiter folgt aus P irreduzibel über K und $P(f) = 0$, daß $N(f - a_1) = P(a_1) = b_1$ ist. Es gibt dann nach Definition von k_1 eine aus mehr als $\Pi_{i=2}^3 k_i$ Elementen bestehende Unterklasse $\mathscr{N}_2 \subset \mathscr{N}_1$, so daß $(f - a_1)R_L = (g - a_1)R_L$ für alle f, $g \in \mathscr{N}_2$ ist. Entsprechend erhalten wir über $N(f - a_2) = P(a_2) = b_2$ eine Unterklasse $\mathcal{N}_3 \subset \mathcal{N}_2$ usw., so daß es schließlich $f, g \in \mathcal{N}_1(b)$ mit $f \neq g$ und $(f - a_i)R_L = (g - a_i)R_L$ für $1 \leqslant i \leqslant 3$ gibt.

Da für zwei verschiedene $b = (b_1, b_2, b_3) \neq \tilde{b} = (\tilde{b}_1, \tilde{b}_2, \tilde{b}_3)$ natürlich $\mathcal{N}_1(b) \cap \mathcal{N}_1(\tilde{b}) = \varnothing$ ist, folgt mit Satz 1, daß es nur endlich viele b gibt, so daß die Abschätzung in Satz 4 falsch ist.

In der Situation von Satz 4 genügen übrigens schon 2 Werte $a_1 \neq a_2$, so daß $\{P \in \mathcal{M}; P(a_i) = b_i$ für $1 \leqslant i \leqslant 2\}$ endlich ist. Entscheidend ist aber die Abschätzung für die Mächtigkeit in Satz 4, die insbesondere bei nachstehender Folgerung eingeht:

FOLGERUNG 5. Sei $L \supset \mathbb{Q}$ ein Zahlkörper mit $n = [L:\mathbb{Q}]$. Weiter seien a_1, a_2, a_3 drei verschiedene Elemente aus $\mathbb{Z}$, die nicht eine arithmetische Progression bilden.

Dann gibt es für fast alle Primzahltripel (p_1, p_2, p_3) höchstens n^3 viele normierte irreduzible Polynome $P \in \mathbb{Z}[X]$ vom Grad n mit $P(a_i) = p_i$ für $1 \leqslant i \leqslant 3$, so daß es ein $a \in L$ mit $P(a) = 0$ gibt.

Übrigens darf hier in Folgerung 5 durchaus $a_1 = \frac{1}{2}(a_2 + a_3)$ sein, wenn stattdessen gefordert wird, daß die erste Primzahl p_1 groß genug ist. (Denn wenn $(f - a_i)R_L = (g - a_i)R_L$ für $1 \leqslant i \leqslant 3$ und $f \neq g$ mit $f, g \in R_L$ gilt, bleibt nach Gegenbeispiel 3 nur der Fall $f = (a_2 - a_1)e + a_1$ übrig. Dann ist $N(f - a_1) \in (a_2 - a_1)R_K^*$, womit $p_1 = P(a_1) \in (a_2 - a_1)R_K^*$ folgt.)

LITERATUR

1. Evertse, J. M.: On sums of S-units and linear recurrences. *Compos. Math.* 53, 225–244 (1984).
2. Langmann, K.: Anwendungen des Satzes von Picard. *Math. Ann.* 266, 369–390 (1984).
3. Laurent, M.: Equations diophantiennes exponentielles. *Invent. Math.* 78, 299–327 (1984).
4. Nevanlinna, R.: *Le théorème de Picard-Borel et la théorie des functions méromorphs.* New York: Chelsea 1974.
5. van der Poorten, A. J. and Schlickewei, H. P.: The growth conditions for recurrence sequences. *Macquarie Math. Rep.* 82-0041; North-Ryde, Australia (1982).