

Bemerkungen über Iterierten von Polynomen

Von JÁNOS FEHÉR (Pécs)

1. Es sei $f(x)$ eine beliebige komplexwertige Funktion einer komplexen Variablen, und

$$f_1(x) = f(x), \quad f_k(x) = f(f_{k-1}(x)), \quad \text{für } k = 2, 3, \dots$$

Die komplexe Zahl α wird *Fixpunkt* von $f(x)$ genannt, falls $f_\mu(\alpha) = \alpha$, (μ ganze positiv) gilt. Die Ordnung des Fixpunktes α ist μ , falls μ die kleinste Zahl mit dieser Eigenschaft ist. Wenn α ein Fixpunkt von der Ordnung $\mu > 1$ ist, dann sind die komplexen Zahlen $\alpha_1 = f(\alpha)$, $\alpha_2 = f_2(\alpha)$, ..., $\alpha_\mu = f_\mu(\alpha)$ paarweise verschiedene Fixpunkte von der Ordnung μ , $\{\alpha, \alpha_1, \dots, \alpha_{\mu-1}\}$ ist ein *Zyklus* von der Ordnung μ . Verschiedene Zyklen haben keine gemeinsamen Punkte. Die Fixpunkte, die zu demselben Zyklus gehören, werden zusammengehörige Fixpunkte genannt [1]¹⁾.

Sämtliche in dieser Arbeit auftretenden Einheitswurzeln sind $\neq 1$, was wir in der Folge nicht besonders erwähnen werden.

Die Verallgemeinerung einer Fragestellung von J. BINZ [2] hat zum folgenden Problem geführt:

Es sei $s > 1$ eine gegebene ganze Zahl. Man bestimme alle Zyklen von der Ordnung μ des Polynoms $f(x) = x^s$ ($\mu = 1, 2, \dots$).

Das folgende Problem stammt von ZOLTÁN DARÓCZY und IMRE KÁTAI:

Es sei $g(x)$ ein beliebiges Polynom (vom Grad mindestens zwei) mit komplexen Koeffizienten. Unter welchen Bedingungen bezüglich g oder μ hat g ein Zyklus von der Ordnung μ ?

2. Von nun an bezeichnet g ein Polynom mit komplexen Koeffizienten. Der Index von g (und nur dieser) bezeichnet immer die entsprechende Iterierte von $g(x)$.

Lemma 1. *Ist die komplexe Zahl α eine Lösung der Gleichung*

$$(1) \quad g_n(x) - x = 0,$$

dann ist α ein Fixpunkt von g , dessen Ordnung ein Teiler von n ist.

BEWEIS. Wenn α die Gleichung (1) erfüllt, dann ist α ein Fixpunkt gemäß der Definition. Es sei μ die Ordnung von α . Dann gilt offenbar $\mu \leq n$, und deshalb

¹⁾ In der Iterationstheorie ([1]) werden die Zusammengehörigen Fixpunkte konjugierte Fixpunkte genannt. Hier aber sind die Fixpunkte komplexe Zahlen, und die Bezeichnung „konjugiert“ könnte zu einem Mißverständnis führen.

$n = k\mu + t$ (k und t sind ganze Zahlen) wo $k \geq 1$ und $0 \leq t < \mu$ gelten. Nehmen wir im Gegenteil an, daß $t > 0$ ist. Dann folgt $\alpha = g_t(g_{k\mu}(\alpha)) = g_t(\alpha)$, und diese Gleichung widerspricht der Minimalität von μ . ■

Wenn die komplexe Zahl α die Gleichung (1) erfüllt, dann bezeichne $m_n(\alpha)$ die Multiplizität der Nullstelle des Polynoms $g_n(x) - x$; es gilt $m_n(\alpha) = 0$, falls $g_n(\alpha) - \alpha \neq 0$.

Satz 1. Wenn α_1 und α_2 zusammengehörige Fixpunkte von g sind, dann gilt $m_n(\alpha_1) = m_n(\alpha_2)$ für alle n .

Wir lassen den folgenden Hilfssatz vorausgehen:

Lemma 2. Es sei $H^{(0)}(x) = H(x) = g_n(x) - x$ und es bezeichne $H^{(i)}(x)$ die Ableitung i -ter Ordnung von $H(x)$ für $i > 0$. Es sei $k \geq 1$. Für $H^{(i)}(\alpha) = H^{(i)}(g(\alpha)) = 0$ ($i = 0, 1, \dots, k-1$), und $H^{(k)}(\alpha) = 0$ gilt $H^{(k)}(g(\alpha)) = 0$.

BEWEIS. Nehmen wir an, dass die Voraussetzungen des Hilfssatzes erfüllt sind, und bezeichnen wir die Menge aller Polynome mit komplexen Koeffizienten mit $C[x]$. Für $f, q \in C[x]$ ist $q(x) - x$ ein Teiler von $f(q(x)) - f(x)$, und hieraus ergibt sich

$$H(g(x)) = g_n(g(x)) - g(x) = g(g_n(x)) - g(x) = (g_n(x) - x)R(x)$$

und

$$(2) \quad H(g(x)) = H(x)R(x) \quad (R \in C[x]).$$

Die k -te Ableitung der linken Seite von (2) ist

$$(3) \quad H^{(k)}(g(x)) \cdot (g'(x))^k + \sum_{i=0}^{k-1} H^{(i)}(g(x)) \cdot K_i(x),$$

wobei $K_i \in C[x]$ ($K_0 \equiv 0$).

Die k -te Ableitung der rechten Seite ist

$$(4) \quad \sum_{i=0}^k \binom{k}{i} H^{(i)}(x) R^{(k-i)}(x).$$

Durch Vergleich von (3) und (4) folgt nach der Substitution $x = \alpha$

$$H^{(k)}(g(\alpha)) \cdot (g'(\alpha))^k = 0.$$

Wir haben aber $H'(\alpha) = (g_{n-1})'(g(\alpha)) \cdot g'(\alpha) - 1 = 0$, für $n > 1$, und $H'(\alpha) = g'(\alpha) - 1 = 0$ für $n = 1$, und hieraus folgt $g'(\alpha) \neq 0$. Damit ist das Lemma bewiesen. ■

BEWEIS DES SATZES 1. Setzen wir voraus, daß $m_n(\alpha_1) \geq m_n(\alpha_2)$ und $m_n(\alpha_1) \geq 1$ ist. Da α_1 und α_2 zusammengehörigende Fixpunkte sind, folgt $\alpha_2 = g_r(\alpha_1)$ für ein $r < \mu$. Nach Lemma 2. gilt:

$$m_n(\alpha_1) \leq m_n(g(\alpha_1)) \leq \dots \leq m_n(g_r(\alpha_1)) = m_n(\alpha_2).$$

Damit folgt die Behauptung $m_n(\alpha_1) = m_n(\alpha_2)$ aus unserer Voraussetzung.

Satz 2. Es sei α ein Fixpunkt erster Ordnung von g . Die Beziehung $m_n(\alpha) > m_1(\alpha)$ ist dann und nur dann richtig, wenn $g'(\alpha)$ ein n -ter Einheitswurzel ist.

BEWEIS. Es sei $h_n(x) \in C[x]$ definiert durch die Relation

$$(5) \quad g_{n+1}(x) - g(x) = (g_n(x) - x)h_n(x) \quad (n = 1, 2, \dots).$$

Es ist leicht zu sehen, daß

$$(6) \quad h_n(x) = g'(x) \pmod{(g_n(x) - x)}$$

gilt. Aus (5) gewinnt man

$$g_n(x) - x = h_{n-1}(x)(g_{n-1}(x) - x) + (g(x) - x),$$

und daraus folgt

$$(7) \quad g_n(x) - x = (g(x) - x)(1 + h_{n-1} + \dots + h_1 \cdot h_2 \dots h_{n-1}).$$

Man beachte, daß $g(x) - x \mid g_n(x) - x$ und $0 < m_1(\alpha) \leq m_n(\alpha)$ für alle n gelten, und daß aus (6)

$$h_n(\alpha) = g'(\alpha) \quad (n = 1, 2, \dots)$$

folgt. Wegen der Gleichung (7) gilt die Relation $0 < m_1(\alpha) < m_{3n}(\alpha)$ dann und nur dann, wenn

$$1 + h_{n-1}(\alpha) + \dots + h_1(\alpha) \cdot h_2(\alpha) \dots h_{n-1}(\alpha) = 0,$$

d.h.

$$1 + g'(\alpha) + \dots + (g'(\alpha))^{n-1} = 0$$

ist. Damit ist der Satz bewiesen. ■

Folgerungen

Für $d \mid n$ gilt $g_d(x) - x \mid g_n(x) - x$, und somit $m_n(\alpha) \geq m_d(\alpha)$.

Folgerung 1. Es sei α ein Fixpunkt d -ter Ordnung von g , und $d \mid n$. Die Relation $m_d(\alpha) < m_n(\alpha)$ gilt genau dann, wenn $(g_d)'(\alpha)$ ein n/d -ter, Einheitswurzel ist.

Dies folgt unmittelbar aus dem Satz 2., mit g_d statt g .

Folgerung 2. Wenn für alle Teiler $d < n$ von n (> 1) und für alle Fixpunkte d -ter Ordnung α von g , $(g_d)'(\alpha)$ ein n/d -ter Einheitswurzel ist, dann hat g mindestens einen Zyklus n -ter Ordnung.

BEWEIS. Es sei $\bar{m}_d(\alpha) = m_d(\alpha)$, falls α ein Fixpunkt d -ter Ordnung ist, und $\bar{m}_d(\alpha) = 0$ andernfalls. Ferner sei

$$\bar{G}_d = \sum_{\alpha} \bar{m}_d(\alpha).$$

(Summation für alle Fixpunkte d -ter Ordnung.) Ferner sei s (> 1) der Grad von g . Dann folgt aus Lemma 1 und aus Satz 2;

$$S^d = \sum_{\delta \mid d} \bar{G}_{\delta} \quad (\forall d \mid n),$$

und aus der Moebiuschen Inversionformel ergibt sich die Gleichung

$$(8) \quad \bar{G}_n = \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot S^d.$$

(Hier bezeichnet μ die Moebiusfunktion)) Aus (8) erhält man

$$\bar{G}_n \equiv S^n - \sum_{d=1}^{n-1} S^d > 0,$$

womit die Behauptung bewiesen ist. ■

3. Bemerkungen

1. Aus Satz 1 folgt, daß für beliebiges g und n die Summe $\bar{G}_n$ der Multiplizitäten der Fixpunkte n -ter Ordnung durch n teilbar ist.

2. Es sei $g(x) = x^s$ ($s > 1$). Dann ist jede Nullstelle des Polynoms $g_n(x) - x$ einfach. In diesem Fall bezeichne $G(n)$ bzw. $M(n)$ die Zahl der Fixpunkte n -ter Ordnung, bzw. der Zykeln n -ter Ordnung. Dann gilt offenbar $M(n) = G(n)/n$ und

$$(9) \quad G(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) S^d \quad (n = 2, 3, \dots; s = 2, 3, \dots).$$

Aus (9) gewinnt man leicht die Gaussche Verallgemeinerung des Fermatschen Satzes²⁾.

3. Es seien α_1 , und α_2 verschiedene komplexe Zahlen und

$$g(x) = x + \frac{2}{\alpha_2 - \alpha_1} (x - \alpha_1)(x - \alpha_2).$$

Dann hat g keinen Fixpunkt zweiter Ordnung. Es gilt nämlich $g'(\alpha_1) = -1$ und aus Satz 2 folgt $m_2(\alpha_1) > 1$, sowie $m_2(\alpha_2) \equiv 1$. Gäbe es einen Fixpunkt zweiter Ordnung, dann gäbe es deren zwei, aber wegen $\deg g_2 = 4$ ist das unmöglich. (Aus $g'(\alpha_2) = 3$ folgt $g_2(x) = x + A(x - \alpha_1)^3(x - \alpha_2)$.)

4. Wenn jede Nullstelle des Polynomes $g(x) - x$ mindestens die Multiplizität zwei hat und p eine Primzahl ist, dann hat g ein Zyklus p -ter Ordnung. (Die Bedingungen der Folgerung 2 sind erfüllt.)

5. Es sei p eine Primzahl, $s > 1$ und $\alpha \neq 0$. Ferner sei

$$g(x) = x + x^s(x - \alpha).$$

Aus Satz 2 folgt $m_p(0) = s$ und $m_p(\alpha) \equiv 1$. Auf Grund von Satz 1 ist die Summe $\bar{G}_p$ der Multiplizitäten der Fixpunkte p -ter Ordnung durch p teilbar.

²⁾ $\sum_{d|n} \mu\left(\frac{n}{d}\right) S^d \equiv 0 \pmod{n}$ ([3], Seite 226.)

Weil p eine Primzahl bezeichnet, ist die Ordnung jeder Nullstelle von $g_p(x) - x$ eins oder p , und daraus ergibt sich die Gleichung

$$\bar{G}_p = (s+1)^p - s - m_p(\alpha).$$

Aus dem Satz von Fermat erhalten wir $m_p(\alpha) = kp + 1$. Wenn $(\alpha^s + 1)^p = 1$ ist, dann folgt aus Satz 2. $k \geq 1$.

Hiermit möchte der Autor den Professoren BÉLA BARNA, ZOLTÁN DARÓCZY und IMRE KÁTAI für ihre Hilfe bei der Abfassung dieser Arbeit den besten Dank sagen.

Literatur

- [1] B. BARNA, Über die Iteration reeller Funktionen I. *Publ. Math. (Debrecen)*, **7** (1960), 16—40.
- [2] J. BINZ, Aufgabe 817. *Elem. Math.* **34** (1979), 18.
- [3] I. NIVEN—H. S. ZUCKERMAN, Bevezetés a számelméletbe (An introduction to the theory of numbers. Übersetzung: Hajnal Andrásné und Szemerédi Endre), *Műszaki Könyvkiadó, Budapest*, 1978.

(Eingegangen am 16. Oktober 1981)