Ganzwertige Polynome

1. Einführung

Wir betrachten Polynome in einer Veränderlichen x mit rationalen Koeffizienten, also Elemente des Rings $\mathbb{Q}[x]$. Im Folgenden wird die Abbildung

$$\Delta : \mathbb{Q}[x] \to \mathbb{Q}[x] \text{ mit } (\Delta f)(x) = f(x+1) - f(x)$$

eine wichtige Rolle spielen. Offensichtlich ist Δ eine $\mathbb{Q}$-lineare Abbildung.
Wir erweitern Binomialkoeffizienten auf Polynome durch folgende Definition

$$\binom{x}{k} = \frac{x \cdot (x-1) \cdot (x-2) \cdot \dots \cdot (x-(k-1))}{1 \cdot 2 \cdot \dots \cdot k} \text{ für } k \in \mathbb{N} \quad \text{und} \quad \binom{x}{0} = 1.$$

Insbesondere ist

$$\binom{x}{0} = 1, \quad \binom{x}{1} = x, \quad \binom{x}{2} = \frac{1}{2}x(x-1), \quad \binom{x}{3} = \frac{1}{6}x(x-1)(x-2), \quad \dots$$

LEMMA. (1) *Für $k \in \mathbb{N}_0$ hat das Polynom $\binom{x}{k}$ Grad k und höchsten Koeffizienten $\frac{1}{k!}$, also*

$$\binom{x}{k} = \frac{1}{k!}x^k + \dots$$

(2) *Für $n \in \mathbb{N}_0$ bilden*

$$1, x, x^2, \dots, x^n \quad \textit{oder} \quad \binom{x}{0}, \binom{x}{1}, \binom{x}{2}, \dots, \binom{x}{n}.$$

eine Basis des $\mathbb{Q}$-Vektorraums $P_n = \{f(x) \in \mathbb{Q}[x] : \operatorname{grad} f(x) \leq n\}$ der Polynome vom Grad $\leq n$.

(3) *Es gilt*

$$\Delta\binom{x}{0} = 0 \quad \textit{und} \quad \Delta\binom{x}{k} = \binom{x}{k-1} \textit{ für } k \geq 1.$$

Beweis:

(1) Klar.
(2) Klar.

Datei: anazt_ganzwpolynome.tex. Version vom 15.11.2020

(3) Es ist

$$\begin{aligned}
\Delta\binom{x}{0} &= \binom{x+1}{0} - \binom{x}{0} = 1 - 1 = 0,\\
\Delta\binom{x}{1} &= \binom{x+1}{1} - \binom{x}{1} = (x+1) - x = 1 = \binom{x}{0},\\
\Delta\binom{x}{2} &= \binom{x+1}{2} - \binom{x}{2} = \frac{1}{2}(x+1)x - \frac{1}{2}x(x-1) = x = \binom{x}{1},\\
\Delta\binom{x}{k} &= \binom{x+1}{k} - \binom{x}{k} =\\
&\overset{k\geq 2}{=} \frac{(x+1)x(x-1)\dots(x-(k-2))}{k!} - \frac{x(x-1)\dots(x-(k-2))(x-(k-1))}{k!} =\\
&= \frac{x(x-1)\dots(x-(k-2))}{k!}\big((x+1)-(x-(k-1))\big) =\\
&= \frac{x(x-1)\dots(x-(k-2))}{k!}\cdot k = \frac{x(x-1)\dots(x-(k-2))}{(k-1)!} = \binom{x}{k-1}.
\end{aligned}$$

Dies beweist die Behauptung. ■

LEMMA. *Jedes Polynome $f \in \mathbb{Q}[x]$ vom Grad $\leq n$ hat eine eindeutige Darstellung*

$$f = \sum_{i=0}^{n} a_i \binom{x}{i} \quad \textit{mit} \quad a_i \in \mathbb{Q}.$$

Es gilt

$$\Delta^k f = \sum_{i\geq 0} a_{k+i}\binom{x}{i} \quad \textit{und} \quad a_k = (\Delta^k f)(0).$$

(Dabei wird $\Delta^k f$ iterativ durch $\Delta^k f = \Delta(\Delta^{k-1} f)$ definiert.) Insbesondere gilt

$$f = \sum_{i=0}^{n} (\Delta^i f)(0)\binom{x}{i}.$$

Beweis: Die Darstellbarkeit und Eindeutigkeit der Darstellung folgt aus der Tatsache, dass die Polynome $\binom{x}{k}$, $k \geq 0$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}[x]$ bilden. Sei jetzt

$$f = \sum_{i\geq 0} a_i \binom{x}{i}.$$

Mit der $\mathbb{Q}$-Linearität von Δ und $\Delta\binom{x}{i} = \binom{x}{i-1}$ (für $i \geq 1$) erhalten wir

$$\Delta f = \sum_{i\geq 0} a_i \Delta\binom{x}{i} = \sum_{i\geq 1} a_l \Delta\binom{x}{i} = \sum_{i\geq 1} a_i \binom{x}{i-1} = \sum_{i\geq 0} a_{i+1}\binom{x}{i}.$$

Damit erhält man durch Induktion sofort

$$\Delta^k f = \sum_{i\geq 0} a_{k+i}\binom{x}{i}.$$

Setzt man nun $x = 0$ ein, so ergibt sich

$$(\Delta^k f)(0) = a_k,$$

was noch zu zeigen war. ■

Bemerkung: Sei $f \in \mathbb{Q}[x]$ ein Polynom vom Grad n. Kennen wir die Werte $f(0), f(1), \dots, f(n)$, so können wir

$$(\Delta f)(0) = f(1) - f(0), \quad (\Delta f)(1) = f(2) - f(1), \quad \dots, \quad (\Delta f)(n-1) = f(n) - f(n-1)$$

berechnen, damit dann

$$(\Delta^2 f)(0) = (\Delta f)(1) - (\Delta f)(0), \quad \dots \quad (\Delta^2 f)(n-2) = (\Delta f)(n-1) - (\Delta f)(n-2),$$

damit

$$(\Delta^3 f)(0) = (\Delta^2 f)(1) - (\Delta^2 f)(0), \quad \dots, \quad (\Delta^3 f)(n-4) = (\Delta^2 f)(n-2) - (\Delta^2 f)(n-3),$$

und so weiter. An letzter Stelle kommt dann

$$(\Delta^n f)(0) = (\Delta^{n-1} f)(1) - (\Delta^{n-1} f)(0).$$

Schreiben wir

$$a_{i,j} = (\Delta^i f)(j),$$

so gilt

$$a_{0,j} = f(j) \quad \text{und} \quad a_{i+1,j} = a_{i,j+1} - a_{i,j}.$$

Bilden wir damit folgendes Schema

$$\begin{array}{ccccccc} a_{0,0} & a_{0,1} & a_{0,2} & \dots & a_{0,n-2} & a_{0,n-1} & a_{0,n} \\ a_{1,0} & a_{1,1} & a_{1,2} & \dots & a_{1,n-2} & a_{1,n-1} & \\ a_{2,0} & a_{2,1} & a_{2,2} & \dots & a_{2,n-3} & & \\ \vdots & \vdots & \vdots & & & & \\ a_{n-1,0} & a_{n-1,1} & & & & & \\ a_{n,0} & & & & & & \end{array}$$

so erhalten wir

$$f = \sum_{k=0}^{n} a_{k,0} \binom{x}{k}.$$

Beispiel: Wir suchen ein Polynom vom Grad 3 mit $f(0) = 4$, $f(1) = 2$, $f(2) = 5$, $f(3) = 7$. Wir bilden das oben angegebene Schema:

$$\begin{array}{cccc} 4 & 2 & 5 & 7 \\ -2 & 3 & 2 & \\ 5 & -1 & & \\ -6 & & & \end{array}$$

und erhalten damit das gesuchte Polynom:

$$f = 4 - 2\binom{x}{1} + 5\binom{x}{2} - 6\binom{x}{3} = 4 - \frac{13}{2}x + \frac{11}{2}x^2 - x^3.$$

2. Ganzwertige Polynome

Wir interessieren uns jetzt für Polynome, die an ganzen Stellen ganze Werte annehmen, also für

$$\mathrm{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[x] : f(n) \in \mathbb{Z} \text{ für alle } n \in \mathbb{Z}\} = \{f \in \mathbb{Q}[x] : f(\mathbb{Z}) \subseteq \mathbb{Z}\}.$$

Offensichtlich ist $\mathrm{Int}(\mathbb{Z})$ ein Ring und es gelten die Inklusionen

$$\mathbb{Z}[x] \subseteq \mathrm{Int}(\mathbb{Z}) \subseteq \mathbb{Q}[x].$$

$\mathrm{Int}(\mathbb{Z})$ wird als Ring der ganzwertigen Polynome bezeichnet. Wir schreiben auch manchmal $R = \mathrm{Int}(\mathbb{Z})$.

Beispiel: Da für $n \in \mathbb{Z}$ eine der Zahlen n oder $n+1$ gerade ist, liefert

$$f = \frac{1}{2}x(x+1) = \frac{1}{2}x^2 + \frac{1}{2}x$$

ein Beispiel eines ganzwertigen Polynoms, also $f \in \mathrm{Int}(\mathbb{Z})$, mit $f \notin \mathbb{Z}[x]$, was $\mathbb{Z}[x] \subsetneq \mathrm{Int}(\mathbb{Z})$ zeigt. Offensichtlich gilt aber $\frac{df}{dx} = f' = x + \frac{1}{2} \notin \mathrm{Int}(\mathbb{Z})$, also ist $\mathrm{Int}(\mathbb{Z})$ nicht abgeschlossen unter Differentiation.

Bemerkung: Für $f(x) \in \mathrm{Int}(\mathbb{Z})$ und $a \in \mathbb{Z}$ ist auch $f(x+a) \in \mathrm{Int}(\mathbb{Z})$, außerdem auch $(\Delta f)(x) = f(x+1) - f(x)$.

Das folgende Lemma beschreibt, was passiert, wenn man die Polynome $\binom{x}{n}$ in ganzen Zahlen auswertet.

LEMMA. *Für $n \in \mathbb{N}$ und $m \in \mathbb{Z}$ gilt*

$$\binom{m}{n} = \begin{cases} \binom{m}{n} \in \mathbb{N} & \text{für } m \geq n, \\ 0 & \text{für } 0 \leq m \leq n-1, \\ (-1)^n \binom{|m|+n-1}{n} \in \mathbb{Z} & \text{für } m \leq -1, \end{cases}$$

wobei es sich auf der rechten Seite um gewöhnliche Binomialkoeffizienten handelt.

Beweis: Für $m \geq n$ ist $\binom{m}{n}$ der gewöhnliche Binomialkoeffizient. Aus der Definition von $\binom{x}{n}$ sieht man, dass die Nullstellen genau $0, 1, 2, \ldots, n-1$ sind. Für $m < 0$ gilt

$$\begin{aligned} \binom{m}{n} &= \frac{m(m-1)(m-2)\ldots(m-(n-1))}{n!} = \frac{(-1)^n(-m)(-m+1)(-m+2)\ldots(-m+(n-1))}{n!} = \\ &= \frac{(-1)^n(|m|+n-1)\ldots(|m|+2)(|m|+1)|m|}{n!} = (-1)^n\binom{|m|+n-1}{n}, \end{aligned}$$

wobei es sich bei dem letzten Ausdruck wegen $|m|+n-1 \geq 1+n-1 \geq n$ wieder um den gewöhnlichen Binomialkoeffizienten handelt. ■

Damit erhalten wir unmittelbar den ersten Teil des folgenden Satzes:

SATZ. (1) *Für $n \in \mathbb{N}_0$ gilt*

$$\binom{x}{n} \in \mathrm{Int}(\mathbb{Z}).$$

(2) *Für ein Polynom $f \in \mathbb{Q}[x]$, geschrieben als $f(x) = \sum_{k=0}^{n} a_k \binom{x}{k}$ mit $a_k \in \mathbb{Q}$ gilt:*

$$f \in \mathrm{Int}(\mathbb{Z}) \quad \Longleftrightarrow \quad a_0, a_1, \ldots, a_n \in \mathbb{Z}.$$

Insbesondere:

$$\mathrm{Int}(\mathbb{Z}) = \{f = \sum_{i \geq 0} a_i \binom{x}{i} : a_i \in \mathbb{Z}\}.$$

Beweis: Wir müssen nur noch den zweiten Teil beweisen. Sei $f \in \mathrm{Int}(\mathbb{Z})$. Da $\mathrm{Int}(\mathbb{Z})$ abgeschlossen unter der Δ-Operation ist, folgt $a_k = (\Delta^k f)(0) \in \mathbb{Z}$. Sind $a_0, \ldots, a_n \in \mathbb{Z}$, so ist sofort klar, dass $f \in \mathrm{Int}(\mathbb{Z})$ gilt. ■

3. $\mathrm{ggT}(\{f(k) : k \in \mathbb{Z}\})$

SATZ. *Sei $f \in \mathrm{Int}(\mathbb{Z})$ mit $f = \sum_{k=0}^{n} a_k \binom{x}{k}$ (und $a_k \in \mathbb{Z}$). Dann gilt*

$$\mathrm{ggT}(\{f(k) : k \in \mathbb{Z}\}) = \mathrm{ggT}(f(0), f(1), \ldots, f(n)) = \mathrm{ggT}(a_0, a_1, \ldots, a_n).$$

Beweis:

(1) Sei $d = \mathrm{ggT}(f(0), f(1), \ldots, f(n)$. Durch Induktion sieht man dann, dass auch $d \mid (\Delta^i f)(j)$ für $j = 0, \ldots, n-i$ gilt. gilt. Mit $a_k = (\Delta^k f)(0)$ folgt $d \mid a_k$, also

$$\mathrm{ggT}(f(0), f(1), \ldots, f(n)) \mid \mathrm{ggT}(a_0, a_1, \ldots, a_n).$$

(2) Sei $d = \mathrm{ggT}(a_0, a_1, \ldots, a_n)$. Aus

$$f = \sum_{k=0}^{n} a_k \binom{x}{k}$$

folgt dann sofort $d \mid f(k)$ für alle $k \in \mathbb{Z}$, also

$$\mathrm{ggT}(a_0, a_1, \ldots, a_n) \mid \mathrm{ggT}(\{f(k) : k \in \mathbb{Z}\}).$$

(3) Trivialerweise gilt

$$\mathrm{ggT}(\{f(k) : k \in \mathbb{Z}\}) \mid \mathrm{ggT}(f(0), f(1), \ldots, f(n)).$$

(4) Die Behauptung folgt nun aus (1), (2), (3). ■

FOLGERUNG. *Ist $f \in \mathrm{Int}(\mathbb{Z})$ ein Polynom vom Grad $\leq n$ und $a \in \mathbb{Z}$, so gilt*

$$\mathrm{ggT}(\{f(k) : k \in \mathbb{Z}\} = \mathrm{ggT}(f(a), f(a+1), \ldots, f(a+n)).$$

(Insbesondere gilt die Aussage natürlich für Polynom aus $\mathbb{Z}[x]$.)

Beweis: Wir definieren $g \in \mathbb{Q}[x]$ durch $g(x) = f(x+a)$. Dann ist $g \in \mathrm{Int}(\mathbb{Z})$ und aus $\{g(k) : k \in \mathbb{Z}\} = \{f(k) : k \in \mathbb{Z}\}$ folgt mit dem vorangegangenen Satz, angewandt auf g:

$\mathrm{ggT}(\{f(k) : k \in \mathbb{Z}\}) = \mathrm{ggT}(\{g(k) : k \in \mathbb{Z}\}) = \mathrm{ggT}(g(0), g(1), \ldots, g(n)) = \mathrm{ggT}(f(a), f(a+1), \ldots, f(a+n))$,

was zu zeigen war. ■

Beispiel: Wir betrachten $f(x) = x(x-1)(x-2)\ldots(x-(n-1))$. Es ist $f(0) = f(1) = \cdots = f(n-1) = 0$ und $f(n) = n!$, also sollte $\mathrm{ggT}(\{f(k) : k \in \mathbb{Z}\}) = n!$ gelten. Dies sieht man auch aus der Darstellung

$$f(x) = n! \binom{x}{n}.$$

Beispiel: Für $f = x^2 + x + 2$ gilt

$$\mathrm{ggT}(\{f(k) : k \in \mathbb{Z}\}) = \mathrm{ggT}(f(0), f(1), f(2)) = \mathrm{ggT}(2, 4, 8) = 2.$$