GANZWERTIGE POLYNOME

ZUSAMMENFASSUNG. Wir untersuchen Polynome $f \in \mathbb{C}[X]$, die für alle ganzzahligen Argumente ganzzahlige Werte produzieren, sogenannte *ganzwertige Polynome*. Beispiele für solche Polynome sind durch die sogenannten Binomialpolynome

$$\binom{X}{n} := \frac{X(X-1)\cdots(X-n+1)}{n!}$$

gegeben. Wir sehen, dass sich alle ganzwertigen Polynome in einfacher Weise durch diese Binomialpolynome erzeugen lassen. Wir behandeln dabei [1, S. 10–11, E.10] und schließen mit einigen interessanten Faktorisierungseigenschaften ganzwertiger Polynome, die man in [2] findet.

1. BINOMIALPOLYNOME

1.1. **Definition und erste Eigenschaften.** Wir definieren die *Binomialpolynome* durch

$$P_0 := \binom{X}{0} := 1, \quad P_n := \binom{X}{n} := \frac{X(X-1)\cdots(X-n+1)}{n!} = \frac{1}{n!}\prod_{k=0}^{n-1}(X-k) \tag{1.1}$$

für $n = 1, 2, 3, \ldots$; Das folgende Lemma zeigt zwei einfache Eigenschaften der Binomialpolynome:

Lemma 1.1.

(1) $\binom{X}{n}$ *ist ein Polynom vom Grad* n.

(2) *Für* $n, x \in \mathbb{N}_0$ *mit* $0 \le n \le x$ *ist* $\binom{X}{n}$ *ausgewertet bei* $x =$ *der Binomialkoeffizient* $\binom{x}{n}$.

Beweis. Das folgt sofort aus der Definition (1.1). □

Man beachte, dass der Binoialkoeffizient auf der rechten Seite in Lemma 1.1 (2) nur für $0 \le n \le x$ definiert ist, das Einsetzen von x in das Binomialpolynom auf der linken Seite jedoch für beliebige $x \in \mathbb{Z}$ (oder, allgemeiner: für $x \in \mathbb{C}$) Sinn ergibt.

1.2. **Ganzwertigkeit der Binomialpolynome.** Zur Einstimmung betrachten wir ein Beispiel.

Beispiel 1.2. Das Polynom $P_2 = \binom{X}{2} = \frac{X(X-1)}{2}$ nimmt auf ganzen Zahlen nur ganzzahlige Werte an. In der Tat ist für $x \in \mathbb{Z}$ entweder x oder $x-1$ gerade. Darum ist $x(x-1)/2$ für jedes $x \in \mathbb{Z}$ eine ganze Zahl.

Wir wollen nun das obige Beispiel verallgemeinern.

Satz 1.3. *Sei* $n \in \mathbb{N}_0$. *Dann ist das Polynom* $P_n = \binom{X}{n}$ ganzwertig, *d.h. es ist* $P_n(x) \in \mathbb{Z}$ *für alle* $x \in \mathbb{Z}$.

Der Beweis erfolgt mittels Induktion. Zur Vorbereitung führen wir etwas Notation ein. Für ein Polynom $f \in \mathbb{C}[X]$ sei Δf das Polynom $f(X+1) - f(X)$. Wir erhalten somit eine Abbildung $\Delta\colon \mathbb{Q}[X] \longrightarrow \mathbb{Q}[X]$.

Lemma 1.4. $\Delta\colon \mathbb{C}[X] \to \mathbb{C}[X]$ *ist* $\mathbb{Q}$*-linear, wenn man* $\mathbb{C}[X]$ *in der offensichtlichen Weise als* $\mathbb{C}$*-Vektorraum auffasst. Zudem gilt* $\deg(\Delta f) = (\deg f) - 1$ *für alle* $f \in \mathbb{C}[X] \setminus \{0\}$.

Beweisidee. Nachrechnen. □

Lemma 1.5. *Für* $n \in \mathbb{N}$ *gilt* $\Delta\binom{X}{n} = \binom{X}{n-1}$.

Beweis. Für $n = 1$ ist $\Delta P_1 = P_1(X+1) - P_1 = X + 1 - X = 1 = P_0$. Für $n \ge 2$ hat man

$$\begin{aligned}\Delta\binom{X}{n} &= \binom{X+1}{n} - \binom{X}{n} = \frac{1}{n!}\prod_{k=0}^{n-1}(X+1-k) - \frac{1}{n!}\prod_{k=0}^{n-1}(X-k) \\ &= ([X+1] - [X-n+1])\frac{1}{n!}\prod_{\kappa=0}^{n-2}(X-\kappa) = \frac{1}{(n-1)!}\prod_{\kappa=0}^{(n-1)-1}(X-\kappa) = \binom{X}{n-1}.\end{aligned}$$

□

Beweis von Satz 1.3. Wie angekündigt, führen wir eine Induktion über n. Für $n = 0$ ist $P_0 = 1$ trivialerweise ganzwertig. Sei nun also die Ganzwertigkeit von P_{n-1} bereits für ein $n \in \mathbb{N}$ bewiesen. Wir zeigen nun, dass dann auch P_n ganzwertig ist. Genau genommen zeigen wir mittels Induktion, dass $P_n(x)$ für alle $x = 0, 1, 2, \ldots$ ganzwertig ist; Für negative x lässt sich ähnlich argumentieren. Für $x = 0$ ist die Behauptung dank $P_n(0) = 0 \in \mathbb{Z}$ klar (siehe (1.1)). Sei nun für ein $x \in \mathbb{N}_0$ bereits die Ganzzahligkeit von $P_n(x)$ bekannt. Wegen Lemma 1.5 haben wir $P_n(x+1) - P_n(x) = P_{n-1}(x)$ für alle $x \in \mathbb{Z}$. Der zweite Summand ($P_n(x)$) ist dank unserer Induktionsannahme in der Induktion über x ganzzahlig und $P_{n-1}(x)$ ist dank unserer Induktionsannahme von der Induktion über n als ganzzahlig bekannt. Daraus folgt $P_n(x+1) = P_{n-1}(x) + P_n(x) \in \mathbb{Z}$. □

2. Charakterisierung ganzwertiger Polynome

Wir erinnern an die Definition aus Satz 1.3. Ein Polynom $P \in \mathbb{C}[X]$ heißt *ganzwertig*, wenn $P(x)$ für alle $x \in \mathbb{Z}$ in $\mathbb{Z}$ liegt. Die Menge aller ganzwertigen Polynome wird mit $\mathrm{Int}(\mathbb{Z})$ bezeichnet. Selbstverständlich sind alle Polynome mit ganzzahligen Koeffizienten ganzwertig, d.h. wir haben $\mathbb{Z}[X] \subseteq \mathrm{Int}(\mathbb{Z})$. Andererseits zeigt Beispiel 1.2 bzw. Satz 1.3, dass $\mathrm{Int}(\mathbb{Z})$ echt mehr Polynome enthält als $\mathbb{Z}[X]$. Umgekehrt ist natürlich aber auch nicht jedes Polynom mit rationalen Koeffizienten ganzwertig (z.B. $(1/2)X^0 \notin \mathrm{Int}(\mathbb{Z})$). Wir haben daher eine Inklusionskette

$$\mathbb{Z} \subsetneq \mathbb{Z}[X] \subsetneq \mathrm{Int}(\mathbb{Z}) \subsetneq \mathbb{C}[X]$$

und alle darin auftretenden Inklusionen sind strikt.

2.1. **Charakterisierung über Binomialpolynome.** Die folgende Proposition besagt, dass unsere Betrachtung von Polynomen in $\mathbb{C}[X]$ für die Untersuchung ganzwertiger Polynome unnötig allgemein ist: Es genügt, sich auf Polynome mit rationalen Koeffizienten zu beschränken.

Proposition 2.1. $\mathrm{Int}(\mathbb{Z}) \subsetneq \mathbb{Q}[X]$.

Beweisskizze. Sei $f \in \mathrm{Int}(\mathbb{Z})$. Dann lassen sich die Koeffizienten von f durch Polynominterpolation aus seinen Werten $f(0), f(1), \ldots, f(\deg f)$ rekonstruieren. Da jene Werte nach Voraussetzung alle ganzzahlig sind, liefert die Polynominterpolation allenfalls rationale Koeffizienten. Das zeigt $f \in \mathbb{Q}[X]$. Also gilt $\mathrm{Int}(\mathbb{Z}) \subseteq \mathbb{Q}[X]$. Wegen $(1/2)X^0 \notin \mathrm{Int}(\mathbb{Z})$ ist die Inklusion strikt. □

Man kann leicht nachprüfen, dass es sich bei $\mathrm{Int}(\mathbb{Z})$ tatsächlich um einen Teilring von $\mathbb{Q}[X]$ handelt. In diesem Abschnitt zeigen wir die folgende Charakterisierung ganzwertiger Polynome:

Satz 2.2. *Es ist* $\mathrm{Int}(\mathbb{Z}) = \mathrm{span}_{\mathbb{Z}}\left\{ \binom{X}{n} : n \in \mathbb{N}_0 \right\}$*, d.h. die ganzwertigen Polynome sind genau diejenigen Polynome in* $\mathbb{Q}[X]$*, welche sich als Linearkombination aus den Binomialpolynomen mit ganzzahligen Koeffizienten schreiben lassen.*

2.2. **Beweis von Satz 2.2.** Der Beweis dieses Satzes benötigt noch etwas Vorarbeit, die wir jetzt leisten. Wir definieren nun

$$\Delta^0 := \mathrm{id}_{\mathbb{C}[X]} \quad \text{und} \quad \Delta^k := \underbrace{\Delta \circ \ldots \circ \Delta}_{k \text{ mal}} \quad \text{für } n \in \mathbb{N}.$$

Wir schreiben kurz $\Delta^k f$ für das Bild $\Delta^k(f)$ von f unter der linearen Abbildung Δ^k.

Beispiel 2.3. Für $k \in \mathbb{N}$ ist

$$\Delta(X^k) = (X+1)^k - X^k = \sum_{j=0}^{k-1} \binom{k}{j} X^j = \binom{k}{k-1} X^{k-1} + \ldots = kX^{k-1} + \ldots,$$

wobei „…“ für ein Polynom vom Grad $< k$ steht. Insbesondere folgt hieraus

$$\Delta^k X^k = k! = k\text{-te Ableitung von } X^k \quad \text{und} \quad \Delta^n X^k = 0 = n\text{-te Ableitung von } X^k \quad \text{für} \quad n > k.$$

Für ein Polynom f vom Grad $\leq n$ erhalten wir somit $\Delta^n f = f^{(n)}$.

Lemma 2.4. *Für* $f \in \mathbb{C}[X]$*,* $x \in \mathbb{Z}$ *und* $k \in \mathbb{N}_0$ *ist* $(\Delta^k f)(x) = \sum_{j=0}^{k} \binom{k}{j} (-1)^{k-j} f(x+j)$.

Beweis. Wir betrachten den Verschiebungsoperator $S\colon \mathbb{C}[X] \longrightarrow \mathbb{C}[X]$, $g \mapsto g(X+1)$. Dieser ist offensichtlich linear und wir können Δ als $\Delta = S - \mathrm{id}_{\mathbb{C}[X]}$ schreiben. Also ist Δ^k die k-fache Verkettung von $S - \mathrm{id}_{\mathbb{C}[X]}$. Natürlich

kommutiert S mit $-\mathrm{id}_{\mathbb{C}[X]}$ (d.h. es gilt $S \circ (-\mathrm{id}_{\mathbb{C}[X]}) = (-\mathrm{id}_{\mathbb{C}[X]}) \circ S$). Darum lässt sich der Binomische Lehrsatz im Endomorphismenring $\mathrm{End}(\mathbb{C}[X]) \ni -\mathrm{id}_{\mathbb{C}[X]}, S$ anwenden. Wir erhalten daher

$$\Delta^k = (S - \mathrm{id}_{\mathbb{C}[X]})^k = \sum_{j=0}^{k} \binom{k}{j} S^j \circ (-\mathrm{id}_{\mathbb{C}[X]})^{k-j}.$$

Wegen $(S^j f)(x) = f(x+j)$ erhalten wir daraus schon die Behauptung des Lemmas. □

Proposition 2.5 (Gregory–Newton-Formel)**.** *Für $f \in \mathbb{C}[X]$ vom Grad n gilt $f = \sum_{k=0}^{n} (\Delta^k f)(0) \binom{X}{k}$.*

Beweis. Man rechnet leicht nach, dass es sich bei

$$L\colon \mathbb{C}[X] \longrightarrow \mathbb{C}[X], \quad f \longmapsto \sum_{k=0}^{\deg f} (\Delta^k f)(0) \binom{X}{k},$$

um eine lineare Abbildung handelt. (Dass die obere Summationsgrenze, $\deg f$, vom Argument f von L abhängt, gestaltet den Beweis der Additivitätseigenschaft $L(f+g) = Lf + Lg$, $f, g \in \mathbb{C}[X]$, geringfügig subtiler. Aus Lemma 1.4 folgt allerdings, dass $(\Delta f)^k$ für $k > \deg f$ das Nullpolynom ist. Man darf die Summationsobergrenze also beliebig vergrößern und damit gelingt dann auch der Nachweis der fraglichen Additivität.)

Wir wollen einsehen, dass L die identische Abbildung $\mathrm{id}_{\mathbb{C}[X]}$ ist. Vermöge Linearität genügt es, dies auf einem Erzeugendensystem nachzuweisen. Aus Lemma 1.1 lässt sich folgern, dass die Binomialpolynome $\binom{X}{n}$, $n = 0, 1, 2, \ldots$, ein Erzeugendensystem von $\mathbb{C}[X]$ bilden. (Tatsächlich bilden diese sogar eine Basis.) Der Beweis des Satzes folgt also, wenn wir $L\binom{X}{n} = \binom{X}{n}$ für alle $n \in \mathbb{N}_0$ nachweisen können. Für $n = 0$ sieht man das direkt durch Einsetzen. Für $n \in \mathbb{N}$ bemühen wir Lemma 1.5. Induktiv folgt daraus

$$\Delta^0 \binom{X}{n} = \binom{X}{n}, \quad \Delta^1 \binom{X}{n} = \binom{X}{n-1}, \quad \Delta^2 \binom{X}{n} = \binom{X}{n-2}, \quad \ldots, \quad \Delta^k \binom{X}{n} = \binom{X}{n-k},$$

für $k = 0, 1, 2, \ldots, n$. Für $k < n$ hat $\binom{X}{n-k}$ aber eine Nullstelle bei 0. Darum gilt

$$L\binom{X}{n} = \sum_{k=0}^{n} \left(\Delta^k \binom{X}{n}\right)(0) \binom{X}{k} = \sum_{k=0}^{n} \binom{X}{n-k}(0) \binom{X}{k} = \binom{X}{n-n}(0) \binom{X}{k} = \binom{X}{k}. \qquad \square$$

Beweis von Satz 2.2. Linearkombinationen von Binomialpolynomen mit ganzzahligen Koeffizienten sind gemäß Satz 1.3 jedenfalls ganzwertig. Das beweist die Inklusion $\supseteq$ von der im Satz behaupteten Gleichung. Für die umgekehrte Inklusion müssen wir zeigen, dass ein jedes ganzwertiges Polynom f sich als Linearkombination der Binomialpolynome mit ganzzahligen Koeffizienten schreiben lässt. Dafür wenden wir Proposition 2.5 an und dürfen ohne Beschränkung der Allgemeinheit davon ausgehen, dass f nicht das Nullpolynom ist. Wir sind natürlich fertig, wenn wir $(\Delta^k f)(0) \in \mathbb{Z}$ für alle $k = 0, 1, \ldots, \deg f$ nachweisen können. Das ist aber klar, denn gemäß Lemma 2.4 ist $(\Delta^k f)(0)$ eine Linearkombination von Auswertungen von f bei ganzen Zahlen, gewichtet mit (ganzzahligen!) Binomialkoeffizienten. — Das Ergebnis davon ist natürlich selbst ganzzahlig. □

2.3. **Ein Kriterium für Ganzwertigkeit.** Die nächste Proposition zeigt, dass man ein Polynom auf Ganzwertigkeit überprüfen kann, indem man dieses auf hinreichend vielen (aber endlich vielen!) ganzen Zahlen auswertet.

Proposition 2.6. *Ein Polynom $f \in \mathbb{C}[X]$ vom Grad $n \in \mathbb{N}_0$ ist genau dann ganzwertig, wenn es auf $n+1$ aufeinander folgenden ganzen Zahlen ganzzahlige Werte annimmt.*

Beweis. Sei $f \in \mathbb{C}[X]$ vom Grad $n \in \mathbb{N}_0$ und $a, a+1, \ldots, a+n \in \mathbb{Z}$ mit $f(a), f(a+1), \ldots, f(a+n) \in \mathbb{Z}$. Wir betrachten das Polynom $g = f(a+X)$. Dieses hat ebenfalls Grad n und die Werte $g(0), g(1), \ldots, g(n)$ sind alle ganzzahlig. Aus Proposition 2.5 und Lemma 2.4 (angewendet auf g) folgt, dass g eine Linearkombination von Binomialpolynomen mit ganzzahligen Koeffizienten ist. Also ist g ganzwertig nach Satz 2.2 bzw. gemäß Satz 1.3. Wegen $f = g(X-a)$ erhalten wir daraus aber auch schon die Ganzwertigkeit von f. □

Beispiel 2.7. Wir hatten in Beispiel 1.2 bereits die Ganzwertigkeit des Binomialpolynoms P_2 begründet und jene dann auch in Form von Satz 1.3 in größerer Allgemeinheit bewiesen. Um Proposition 2.6 zu illustrieren, berechnen wir noch

$$P_2(0) = \frac{0(0-1)}{2} = 0, \quad P_2(1) = \frac{1(1-1)}{2} = 0, \quad P_2(2) = \frac{2(2-1)}{2} = 1.$$

Das Polynom P_2 (mit Grad 2) nimmt also auf 3 aufeinander folgenden ganzen Zahlen ganzzahlige Werte an. Proposition 2.6 liefert damit auch die Ganzwertigkeit von P_2. (Das ist aber natürlich kein wirklich unabhängiger Beweis für die Ganzwertigkeit von P_2, da die Ganzwertigkeit der Binomialpolynome, Satz 1.3, schon in den Beweis von Proposition 2.6 eingeflossen ist.)

Beispiel 2.8. Das Polynom $P = (5X + X^3)/6 \in \mathbb{Q}[X]$ ist ganzwertig. Zur Verifikation davon brauchen wir dank Beispiel 1.2 nur feststellen, dass es auf -1, 0, 1 und 2 die Werte -1, 0, 1, respektive 3 annimmt, welche ganzzahlig sind. (Man kann auch $P = P_1 + P_2 + P_3$ verifizieren.)

2.4. **Vergleich von Δ und Differentiation.** Der Ausdruck

$$(\Delta f)(x) = f(x+1) - f(x) = \frac{f(x+1) - f(x)}{(x+1) - x}$$

ist offensichtlich ein Differenzenquotient. Dies legt nahe, dass zwischen Δf und der Ableitung f' von f ein Bezug bestehen könnte. Das folgende Ergebnis bestätigt diesen Verdacht und behandelt auch gleich Δ^k:

Proposition 2.9. *Sei $k \in \mathbb{N}$ und $I := [a, a+k] \subset \mathbb{R}$ ein Intervall. Sei $f\colon I \to \mathbb{R}$ eine k-mal differenzierbare Funktion auf dem Intervall I. Dann gibt es einen Punkt $\xi \in (a, a+k)$ mit $(\Delta^k f)(a) = f^{(k)}(\xi)$.*

Beweis. Durch Polynominterpolation erhalten wir ein (eindeutig bestimmtes) Polynom $p \in \mathbb{R}[X]$ vom Grad $\leq k$, welches an den Stellen $a, a+1, \ldots, a+k$ mit f übereinstimmt.

Wir betrachten die Funktion $g\colon I \to \mathbb{R}$, $x \mapsto f(x) - p(x)$. Diese hat Nullstellen bei den $k+1$ Stellen $a, a+1, \ldots, a+k$. Mit dem aus der Analysis bekannten Satz von Rolle erhalten wir also k Nullstellen von g', welche sich auf die Intervalle zwischen den oben genannten $k+1$ Stellen verteilen. Durch Iteration dieses Verfahrens erhalten wir schließlich eine Nullstelle $\xi \in (a, a+k)$ von $g^{(k)}$. Es gilt also

$$0 = g^{(k)}(\xi) = f^{(k)}(\xi) - p^{(k)}(\xi) = f^{(k)}(\xi) - (\Delta^k p)(\xi) = f^{(k)}(\xi) - (\Delta^k p)(a), \tag{2.1}$$

wobei wir für die vorletzte Gleichung das Ergebnis aus Beispiel 2.3 benutzt haben und für die letzte Gleichung zum Tagen kommt, dass das Polynom $\Delta^k p$ Grad $\leq k - k = 0$ hat und also konstant ist.

Darüber hinaus gilt wegen Lemma 2.4

$$(\Delta^k f)(a) - (\Delta^k p)(a) = (\Delta^k f - \Delta^k p)(a) = (\Delta^k g)(a) = \sum_{j=0}^{k} \binom{k}{j} (-1)^{k-j} g(a+j) = 0.$$

Zusammen mit (2.1) erhalten wir daraus $(\Delta^k f)(a) = (\Delta^k p)(a) = f^{(k)}(\xi)$. □

Bemerkung 2.10. Für eine Anwendung von Proposition 2.9 siehe [1, S. 10–11, E.10, Teil f]. Für die hiesigen Untersuchungen wird Proposition 2.9 aber nicht weiter benötigt.

3. Faktorisierungstheorie in $\mathrm{Int}(\mathbb{Z})$

In Proposition 2.1 hatten wir schon gesehen, dass $\mathrm{Int}(\mathbb{Z})$ in $\mathbb{Q}[X]$ enthalten ist. Tatsächlich kann man leicht nachprüfen, dass es sich bei $\mathrm{Int}(\mathbb{Z})$ um einen Teilring von $\mathbb{Q}[X]$ handelt. Wir wollen im Folgenden sehen, dass der Ring $\mathrm{Int}(\mathbb{Z})$ nicht faktoriell ist. Das benötigt wieder etwas Vorbereitung.

3.1. **Einheiten von $\mathrm{Int}(\mathbb{Z})$.**

Lemma 3.1. $\mathrm{Int}(\mathbb{Z}) \cap \mathbb{Z} = \mathbb{Z}$.

Beweis. Offensichtlich ist jede ganze Zahl aufgefasst als Polynom ganzwertig. Ist umgekehrt ein konstantes Polynom $a = aX^0$ ganzwertig, so folgt durch Auswertung bei 1, dass a in $\mathbb{Z}$ liegt. □

Proposition 3.2. *Die Einheiten von $\mathrm{Int}(\mathbb{Z})$ sind genau die konstanten Polynome ± 1.*

Beweis. Die Polynome ± 1 sind jedenfalls ganzwertig und auch Einheiten. Wir zeigen nun, dass jede Einheit $\epsilon \in \mathrm{Int}(\mathbb{Z})$ gleich 1 oder -1 ist. Sei $\epsilon^{-1} \in \mathrm{Int}(\mathbb{Z})$ das Inverse Element zu ϵ. Aus $1 = \epsilon\epsilon^{-1}$ und der Gradformel folgt $0 = \deg 1 = \deg(\epsilon\epsilon^{-1}) = \deg\epsilon + \deg(\epsilon^{-1})$. Daraus sehen wir, dass ϵ und ϵ^{-1} beide Grad 0 haben. Aus Lemma 3.1 folgt, dass ϵ schon eine Einheit in $\mathbb{Z}$ ist. Also ist $\epsilon \in \{-1, 1\}$. □

3.2. **Einige irreduzible Elemente in $\mathrm{Int}(\mathbb{Z})$.**

Lemma 3.3. *Primzahlen $p \in \mathbb{N}$ sind (aufgefasst als konstante Polynome) irreduzibel in $\mathrm{Int}(\mathbb{Z})$.*

Beweis. Ist $p = ab$ eine Zerlegung von p in Elemente a, b aus $\mathrm{Int}(\mathbb{Z})$, so erkennen wir abermals durch Anwendung der Gradformel, dass a und b selbst konstante Polynome sein müssen. Wegen Lemma 3.1 ist dann sogar $a, b \in \mathbb{Z}$ und weil p laut Annahme in $\mathbb{Z}$ irreduzibel ist, folgt $a = \pm 1$ oder $b = \pm 1$. Also handelt es sich bei a oder bei b um eine Einheit in $\mathbb{Z}$ (und somit *a-fortiori* um eine Einheit in $\mathrm{Int}(\mathbb{Z})$). Also ist p irreduzibel in $\mathrm{Int}(\mathbb{Z})$. □

Lemma 3.4. *Für jedes $a \in \mathbb{Z}$ ist das ganzwertige Polynom $X + a$ irreduzibel in $\mathrm{Int}(\mathbb{Z})$.*

Beweis. Sei $X + a = fg$ eine Faktorisierung von $X + a$ mit Polynomen $f, g \in \mathrm{Int}(\mathbb{Z})$. Aus der Gradformel folgt, dass für die Grade von f und g nur die Kombinationen $(1, 0)$ und $(0, 1)$ in Frage kommen. Ohne Beschränkung der Allgemeinheit sei daher $f = bX + c$ und g ein Konstantes Polynom. Dann ist $X + a = fg = bgX + cg$ und ein Vergleich der Leitkoeffizienten zeigt $bg = 1$. Also ist g eine Einheit. Das zeigt, dass $X + a$ irreduzibel in $\mathrm{Int}(\mathbb{Z})$ ist. □

Satz 3.5. *Für $n \in \mathbb{N}$ ist das Binomialpolynom $P_n = \binom{X}{n}$ irreduzibel in* $\mathrm{Int}(\mathbb{Z})$.

Beweis. Sei $P_n = fg$ eine Faktorisierung von P_n mit Polynomen $f, g \in \mathrm{Int}(\mathbb{Z})$. Schreibe $r = \deg f$, $s = \deg g$. Wegen $n = \deg P_n = \deg(fg) = r + s$ ist $s = n - r$. Gemäß Satz 2.2 ist f eine $\mathbb{Z}$-Linearkombination von $P_0, \ldots, P_r$ und g eine $\mathbb{Z}$-Linearkombination von $P_0, \ldots, P_s$. Aus der Definition (1.1) der Binomialpolynome folgt, dass $r!P_j$ für alle $j \leq r$ ein Polynom mit ganzzahligen Koeffizienten ist. Also ist $r!\, s!\, P_n = (r!f)(s!g) \in \mathbb{Z}$. Der Leitkoeffizient a von $r!\, s!\, P_n$ ist aber

$$a = \frac{r!\, s!}{n!} = \frac{r!\, (n-1)!}{n!} = \binom{n}{r}^{-1}.$$

Weil der hier auftretende Binomialkoeffizient jedoch auch eine (positive) ganze Zahl ist, folgt $a = 1$. Daraus folgt aber schon $r = 0$ oder $r = n$, denn die folgende Rechnung zeigt, dass für andere r die Zahl a nicht 1 sein kann:

$$a = \frac{r!\, s!}{n!} = \frac{r!\, (n-1)!}{n!} = \frac{1 \cdot 2 \cdots r}{n(n-1)\cdots(n-r+1)} = \prod_{j=1}^{r} \frac{j}{n-r+j}.$$

Also hat eines der Polynom f oder g Grad 0. Ohne Beschränkung der Allgemeinheit sei dies g, also $(r, s) = (n, 0)$. Das Argument aus dem Beweis von Lemma 3.4 (Vergleich von Leitkoeffizienten in der Zerlegung $r!\, s!\, P_n = (r!f)(s!g) = (n!f)g$) zeigt, dass g eine Einheit in $\mathrm{Int}(\mathbb{Z})$ ist. □

3.3. **Elastizität und Nicht-Faktorialität von** $\mathrm{Int}(\mathbb{Z})$**.** Sei R nun ein Integritätsbereich in welchem sich jede Nichteinheit $r \in R$, $r \neq 0_R$, als Produkt von (endlich vielen) irreduziblen Elementen schreiben lässt. Sind $p_1 \cdots p_m = q_1 \cdots q_n$ zwei solche Zerlegungen in irreduzible Faktoren von R, so betrachten wir den Buch m/n. Das Supremum über alle derartigen Brüche m/n, die man so aus R erhalten kann, bezeichnet man als die *Elastizität von* R.

Satz 3.6. *Die Elastizität von* $\mathrm{Int}(\mathbb{Z})$ *ist unendlich.*

Beweisskizze. Wir zeigen *nicht*, dass sich jede Nichteinheit $\neq 0$ von $\mathrm{Int}(\mathbb{Z})$ als Produkt von irreduziblen Elementen schreiben lässt. Streng genommen bleibt damit also die Frage, ob die Elastizität von $\mathrm{Int}(\mathbb{Z})$ überhaupt definiert ist, offen. Wir zeigen hier nur, dass es Elemente in $\mathrm{Int}(\mathbb{Z})$ mit Faktorisierungen (in irreduzible Elemente) von sehr unterschiedlicher Länge gibt. Aus der Definition (1.1) der Binomialpolynome erhalten wir für $n \in \mathbb{N}$ leicht die Gleichung

$$n\binom{X}{n} = (X - n + 1)\binom{X}{n-1}.$$

Die beiden Faktoren auf der rechten Seite erkennen wir dank Lemma 3.4 bzw. Satz 3.5 als irreduzibel. Selbiges gilt für den zweiten Faktor auf der linken Seite. Wir wählen nun $n = 2^k$ für $k \in \mathbb{N}$. Dann hat die linke Seite der obigen Gleichung wegen Lemma 3.3 eine Produktzerlegung in $k + 1$ irreduzible Faktoren. □

Korollar 3.7. *Der Ring* $\mathrm{Int}(\mathbb{Z})$ *ist nicht faktoriell.*

Beweis. In einem faktoriellen Ring haben je zwei Faktorisierungen eines Elements in Produkte irreduzibler Elemente dieselbe Anzahl an Faktoren. Somit ist die Elastizität eines jeden faktoriellen Rings gleich 1. Wegen Satz 3.6 kann $\mathrm{Int}(\mathbb{Z})$ also nicht faktoriell sein. □

Bemerkung 3.8. Wir hatten im Beweis von Satz 3.6 zwar nicht geklärt, ob die Elastizität für $\mathrm{Int}(\mathbb{Z})$ tatsächlich definiert ist, aber für die Anwendung auf Korollar 3.7 ist dies tatsächlich unerheblich: Wäre $\mathrm{Int}(\mathbb{Z})$ nämlich faktoriell, so wäre (nach Definition von Faktorialität) auch die Zerlegbarkeit jeder Nichteinheit $\neq 0$ von $\mathrm{Int}(\mathbb{Z})$ in irreduzible Elemente sichergestellt. Der zu Satz 3.6 geführte Beweis führt dann aber auf einen Widerspruch.

LITERATUR

[1] P. Borwein und T. Erdélyi. *Polynomials and polynomial inequalities*. New York, NY: Springer, 1995.

[2] P.-J. Cahen und J.-L. Chabert. What you should know about integer-valued polynomials. *Am. Math. Mon.*, 123(4): 311–337, 2016.