

## Aufgabe 1

**zu zeigen:**  $X^2 + 3X + 2$  ist irreduzibel in  $\mathbb{Z}[[X]]$ , aber reduzibel in  $\mathbb{Z}[X]$

**Beweis:**

Nullstellen von  $X^2 + 3X + 2$ :  $\{-1, -2\}$

Zerlegung:

$$X^2 + 3X + 2 = (X + 1)(X + 2) \quad (1)$$

$X + 1$ ,  $X + 2$  sind keine Einheiten in  $\mathbb{Z}[X]$ , nach Satz 10.5., denn  $\mathbb{Z}$  ist Integritätsring,  $\mathbb{Z}[X]^* = \mathbb{Z}^*$ . Damit ist (1) eine echte Zerlegung in  $\mathbb{Z}[X]$ , und das gegebene Polynom ist reduzibel in  $\mathbb{Z}[X]$ .

Im weiteren untersuche ich  $X^2 + 3X + 2$  in  $\mathbb{Z}[[X]]$ .

$X + 1$  ist eine Einheit in  $\mathbb{Z}[[X]]$ . (Das Inverse zu  $X + 1$  ist  $1 + \sum_{i=1}^{\infty} (-1)^i X^i$ , denn  $(1 + \sum_{i=1}^{\infty} (-1)^i X^i)(X + 1) = X + \sum_{i=1}^{\infty} (-1)^i X^{i+1} + 1 + \sum_{i=1}^{\infty} (-1)^i X^i = X - \sum_{i=2}^{\infty} (-1)^i X^i + 1 + \sum_{i=1}^{\infty} (-1)^i X^i = X + 1 - X = 1$ .)

$X + 2$  ist irreduzibel in  $\mathbb{Z}[[X]]$ , denn 2 ist prim in  $\mathbb{Z}$ , und damit auch irreduzibel, in  $\mathbb{Z}$ , da  $\mathbb{Z}$  Hauptidealring ist.

Folglich ist  $X^2 + 3X + 2$  wegen (1) assoziiert zum irreduziblen Polynom  $X + 2$ , und ist damit irreduzibel in  $\mathbb{Z}[[X]]$ .

## Aufgabe 2

**gegeben:**  $f \in \mathbb{Z}[X]$ ,  $\deg f = 2k + 1$ ,  $f$  habe an  $2k + 1$  Stellen den Wert 1

**zu zeigen:**  $f$  ist irreduzibel

**Beweis:**

Angenommen,  $f$  ist darstellbar als  $f = gh$ . Sei o.B.d.A.  $\deg g \leq \deg h$ . Wir haben  $\deg g + \deg h = \deg f = 2k + 1$  (da Integritätsring), damit sogar  $\deg g < \deg h$ , da  $\deg f$  ungerade,  $\deg g \leq k$ .

Da laut Voraussetzung  $f$  an  $2k + 1$  Stellen den Wert 1 hat, muß  $g$  an  $2k + 1$  Stellen den Wert einer Einheit in  $\mathbb{Z}$  haben, also an  $2k + 1$  Stellen den Wert  $\pm 1$  haben.

Dann hat  $g$  an mindestens  $k + 1$  Stellen den gleichen Wert ( $+1$  oder  $-1$ ), nach Satz 10.9. ( $\mathbb{Z}$  ist Integritätsring mit 1) muß  $g$  konstant 1 sein oder konstant  $-1$ ,  $g$  ist Einheit,  $f$  ist also irreduzibel. ■

### Aufgabe 3

**Voraussetzung:**  $R$  sei faktorieller Ring,  $P$  Primideal in  $R[X]$ ,  $P \cap R = \{0\}$

**Behauptung:**  $P$  ist ein Hauptideal

**Beweis:**

Da  $P$  Primideal in  $R[X]$  ist, ist nach Satz 6.8.  $R[X]/P$  ein Integritätsbereich. Betrachte den kanonischen Homomorphismus  $\varphi : R[X] \rightarrow R[X]/P$ . Nach Voraussetzung ist  $\varphi|_R$  injektiv, da  $P \cap R = \{0\}$ .

Wähle ein Polynom  $f \in P \setminus \{0\}$  mit minimalem Grad. Man kann annehmen, daß  $f$  primitiv gewählt werden kann. Denn wenn  $f = rg$ ,  $r \in R$ ,  $g \in R[X]$  primitiv, dann wegen  $f \in P$   $\varphi(f) = 0$ , und da  $\varphi$  Homomorphismus  $\varphi(f) = \varphi(r)\varphi(g)$ , wegen  $r \in R$ ,  $R \cap P = \{0\}$  ist  $\varphi(r) \neq 0$  ( $f \neq 0$ ), also  $\varphi(g) = 0$  (Integritätsbereich), damit  $g \in P$ . Sei also im weiteren o.B.d.A.  $f$  primitiv. Ich zeige, daß  $P = (f)$ .

Sei also  $g$  ein beliebiges Polynom aus  $P \setminus \{0\}$ . Bezeichne  $K$  den Quotientenkörper von  $R$ . In  $K[X]$ , kann man mit Rest dividieren, denn Polynomringe über einem Körper sind euklidisch. Es gibt also  $q, r \in K[X]$  mit  $g = qf + r$ , und entweder  $r = 0$  oder  $\deg r < \deg f$ .

Wenn  $r \neq 0$ , dann gibt es ein  $a \in R$  mit  $aq \in R[X]$ , und somit  $ag = aqf + ar$ , es folgt  $ag - aqf = ar \in P$ , da  $f, g \in P$ , es ergibt sich ein Widerspruch zur Minimalität von  $f$ .

Also ist  $r = 0$ ,  $g = qf$ . Ich betrachte  $q$ . Seien die Koeffizienten von  $q$  gekürzt, sei  $b$  das kleinste gemeinsame Vielfache der Nenner der Koeffizienten von  $q$ , dann  $aq = bq'$ ,  $q' \in R[X]$  primitiv,  $\text{ggT}(a, b) = 1$ . Es folgt  $ag = bq'f$ . Nach dem Lemma von Gauß ist das Produkt primitiver Polynome wieder primitiv, es folgt  $aI(g) = b$ . Wegen  $a, b$  teilerfremd folgt  $b \mid I(g)$ ,  $a \in R^*$ ,  $g = a^{-1}bq'f$ , folglich  $g \in (f)$ .

$P$  ist also ein Hauptideal. ■

## Aufgabe 4

gegeben:

$$P_0(X) := 1, \quad P_{n+1}(X) := \frac{1}{n+1}(X-n)P_n(X), \quad n \in \mathbb{N} \quad (2)$$

1. zu zeigen:  $P_{n+1}(X+1) = P_n(X) + P_{n+1}(X)$

Aus (2) folgt

$$P_{n+1}(X) = \frac{1}{(n+1)!} \prod_{i=0}^n (X-i). \quad (3)$$

Mittels (3) berechne ich

$$\begin{aligned} P_{n+1}(X+1) - P_{n+1}(X) &= \frac{1}{(n+1)!} \prod_{i=0}^n (X+1-i) - \frac{1}{(n+1)!} \prod_{i=0}^n (X-i) \\ &= \frac{1}{(n+1)!} \left( \prod_{i=0}^n (X-(i-1)) - \prod_{i=0}^n (X-i) \right) \\ &= \frac{1}{(n+1)!} \left( \prod_{i=-1}^{n-1} (X-i) - \prod_{i=0}^n (X-i) \right) \\ &= \frac{1}{(n+1)!} \left( (X+1) \prod_{i=0}^{n-1} (X-i) - (X-n) \prod_{i=0}^{n-1} (X-i) \right) \\ &= \frac{1}{(n+1)!} (X+1 - X+n) \prod_{i=0}^{n-1} (X-i) \\ &= \frac{1}{(n+1)!} (n+1) \prod_{i=0}^{n-1} (X-i) \\ &= \frac{1}{n!} \prod_{i=0}^{n-1} (X-i) \\ &= P_n(X) \end{aligned}$$

nach (3), und die Behauptung ist gezeigt.

2. zu zeigen: für jedes  $a \in \mathbb{Z}$  und jedes  $n \in \mathbb{N}$  ist  $P_n(a) \in \mathbb{Z}$

Der Beweis erfolgt durch vollständige Induktion nach  $n$ .

Induktionsanfang: Für  $n = 0$  ist nach Definition  $P_0(a) = 1 \in \mathbb{Z}$  für beliebiges  $a \in \mathbb{Z}$ .

Induktionsschritt: gelte die Behauptung für gewisses  $n \in \mathbb{N}$ , sei also  $P_n(a) \in \mathbb{Z}$  für alle  $a \in \mathbb{Z}$ . Nach Aufgabenteil 1. gilt

$$P_n(a) = P_{n+1}(a+1) - P_{n+1}(a) \in \mathbb{Z}. \quad (4)$$

Aus (3) folgt  $P_{n+1}(0) = 0$ , mit (4) ergibt sich sukzessive  $P_{n+1}(a) \in \mathbb{Z}$  für ganze Zahlen  $a$ .