

1 | Polynomdivision

Für welche der folgenden Paare von Polynomen A, B existiert in $\mathbb{Z}[X]$ eine Darstellung $A = QB + R$ mit $\deg(R) < \deg(B)$? Bestimmen Sie in diesen Fällen Q und R !

- (a) $A = X^7 + 3X^5 + 7X^4 + X^3 + X + 1, \quad B = X^3 + X + 1$
(b) $A = X^3 + X + 1, \quad B = X^7 + 3X^5 + 6$
(c) $A = X^8 + 4X^7 + 7X^4 - X^3 - X^2 - 1, \quad B = 2X^2 - 2X + 2$

Alle diese Polynome lassen sich auch als Elemente von $\mathbb{Q}[X]$ auffassen. Für welche der Polynome A und B existiert in $\mathbb{Q}[X]$ eine Darstellung $A = QB + R$ mit $\deg(R) < \deg(B)$? Bestimmen Sie auch in diesen Fällen Q und R !

(a) über $\mathbb{Z}$:

$$\begin{array}{r} (X^7 + 3X^5 + 7X^4 + X^3 + X + 1) : (X^3 + X + 1) = \boxed{X^4 + 2X^2 + 6X - 1} \\ - (X^7 + X^5 + X^4) \\ \hline 2X^5 + 6X^4 + X^3 + X + 1 \\ - (2X^5 + 2X^3 + 2X^2) \\ \hline 6X^4 - X^3 - 2X^2 + X + 1 \\ - (6X^4 + 6X^2 + 6X) \\ \hline -X^3 - 8X^2 - 5X + 1 \\ - (-X^3 - X - 1) \\ \hline \boxed{-8X^2 - 4X + 2} \end{array}$$

Q

R

über $\mathbb{Q}$: Rechnung wie über $\mathbb{Z}$, mit demselben Ergebnis.

(b) über $\mathbb{Z}$: $Q = 0, \quad R = A$

über $\mathbb{Q}$: $Q = 0, \quad R = A$

(c) über $\mathbb{Z}$: keine Division möglich, da
 (Leitkoeff. von B) = $2 \notin \mathbb{Z}^+$.

über $\mathbb{Q}$:

$$\begin{array}{r}
 \text{Q } \boxed{\frac{1}{2}x^6 + \frac{5}{2}x^5 + 2x^4 - \frac{1}{2}x^3 + x^2 + x - \frac{1}{2}} \\
 (x^8 + 4x^7 + 7x^4 - x^3 - x^2 - 1) : (2x^2 - 2x + 2) \\
 \underline{-(x^8 - x^7 + x^6)} \\
 5x^7 - x^6 + 7x^4 - x^3 - x^2 - 1 \\
 \underline{-(5x^7 - 5x^6 + 5x^5)} \\
 4x^6 - 5x^5 + 7x^4 - x^3 - x^2 - 1 \\
 \underline{-(4x^6 - 4x^5 + 4x^4)} \\
 -x^5 + 3x^4 - x^3 - x^2 - 1 \\
 \underline{-(-x^5 + x^4 - x^3)} \\
 2x^4 - x^2 - 1 \\
 \underline{-(2x^4 - 2x^3 + 2x^2)} \\
 2x^3 - 3x^2 - 1 \\
 \underline{-(2x^3 - 2x^2 + 2x)} \\
 -x^2 - 2x - 1 \\
 \underline{-(-x^2 + x - 1)} \\
 \text{R } \boxed{-3x}
 \end{array}$$

2 | Ecce homo II

Wir werden in Def. 4.12 der Vorlesung sehen: Eine Abbildung $f: V \rightarrow W$ zwischen zwei K -Vektorräumen $(V, +, \odot)$ und $(W, +, \odot)$ ist **K -linear**, falls für alle $\mathbf{v}, \mathbf{v}_1, \mathbf{v}_2 \in V$ und alle $r \in K$ gilt $f(\mathbf{v}_1 + \mathbf{v}_2) = f(\mathbf{v}_1) + f(\mathbf{v}_2)$ und $f(r \odot \mathbf{v}) = r \odot f(\mathbf{v})$.

Welche der folgenden Abbildungen sind $\mathbb{R}$ -linear?

(a) $\mathbb{R} \rightarrow \mathbb{R}$ nicht linear, denn $0 \mapsto 2 \neq 0$
 $x \mapsto 2 - 3x$

(b) $\mathbb{R} \rightarrow \mathbb{R}$ nicht linear, denn:
 $x \mapsto x^3 - x^2$

$$\begin{array}{ccc} 1 & \mapsto & 0 \\ + & & + \\ 1 & \mapsto & 0 \\ \parallel & & \neq \\ 2 & \mapsto & 4 \end{array}$$

(c) $\mathbb{R}^2 \xrightarrow{f} \mathbb{R}^2$ linear:
 $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} y \\ x \end{pmatrix}$

$$\begin{aligned} f\left(\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} x' \\ y' \end{pmatrix}\right) &= f\left(\begin{pmatrix} x+x' \\ y+y' \end{pmatrix}\right) \\ &= \begin{pmatrix} y+y' \\ x+x' \end{pmatrix} = \begin{pmatrix} y \\ x \end{pmatrix} + \begin{pmatrix} y' \\ x' \end{pmatrix} \\ &= f\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) + f\left(\begin{pmatrix} x' \\ y' \end{pmatrix}\right) \end{aligned}$$

$$f\left(r \cdot \begin{pmatrix} x \\ y \end{pmatrix}\right) = f\left(\begin{pmatrix} rx \\ ry \end{pmatrix}\right) = \begin{pmatrix} ry \\ rx \end{pmatrix} = r \cdot \begin{pmatrix} y \\ x \end{pmatrix} = r \cdot f\left(\begin{pmatrix} x \\ y \end{pmatrix}\right)$$

für alle $r \in K$.

(d) $\mathbb{R}^2 \rightarrow \mathbb{R}$ nicht linear, denn:
 $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{cases} x^2/y & \text{falls } y \neq 0 \\ 0 & \text{falls } y = 0 \end{cases}$

$$\begin{array}{ccc} \begin{pmatrix} 1 \\ 0 \end{pmatrix} & \mapsto & 0 \\ + & & + \\ \begin{pmatrix} 1 \\ 1 \end{pmatrix} & \mapsto & 1 \\ \parallel & & \neq \\ \begin{pmatrix} 2 \\ 1 \end{pmatrix} & \mapsto & 4 \end{array}$$

$$(e) \mathbb{R}[X] \xrightarrow{f} \mathbb{R}[X]$$

$$A \mapsto X^2 \cdot A$$

linear:

$$\begin{aligned} f(A+B) &= X^2 \cdot (A+B) \\ &= X^2 \cdot A + X^2 \cdot B \\ &= f(A) + f(B) \end{aligned}$$

$$\begin{aligned} f(r \cdot A) &= X^2 \cdot (r \cdot A) \\ &= r \cdot X^2 \cdot A \\ &= r \cdot f(A) \end{aligned} \quad \text{für } r \in K$$

$$(f) \mathbb{R}[X] \xrightarrow{f} \mathbb{R}$$

$$A \mapsto A(7)$$

linear:

$$\text{Für } r \in \mathbb{R}, \quad \left. \begin{aligned} A &= \sum_{i=0}^n a_i X^i \\ B &= \sum_{i=0}^m b_i X^i \end{aligned} \right\} \in \mathbb{R}[X] \quad \text{gilt:}$$

$$\begin{aligned} f(A+B) &= f\left(\sum_{i=0}^{\max(n,m)} (a_i + b_i) X^i\right) \\ &= \sum_{i=0}^{\max(n,m)} (a_i + b_i) 7^i \end{aligned}$$

Distributivität
in $\mathbb{R}$ $\Rightarrow$

$$= \sum_{i=0}^{\max(n,m)} (a_i 7^i + b_i 7^i)$$

$$= \sum_{i=0}^{\max(n,m)} a_i 7^i + \sum_{i=0}^{\max(n,m)} b_i 7^i$$

$$= f(A) + f(B)$$

$$f(r \cdot A) = f\left(\sum_{i=0}^n r \cdot a_i X^i\right)$$

$$= \sum_{i=0}^n r \cdot a_i 7^i$$

$$= r \left(\sum_{i=0}^n a_i 7^i \right)$$

$$= r \cdot f(A)$$

$$(g) \mathbb{R}[X] \xrightarrow{ev} \text{Abb}(\mathbb{R}, \mathbb{R})$$

$$A \mapsto ev(A): (x \mapsto A(x))$$

(linear:

Für $A, B \in \mathbb{R}[X]$, $r \in \mathbb{R}$ gilt:

- $ev(A+B) = ev(A) + ev(B)$, denn für jedes $x \in \mathbb{R}$ gilt:

$$ev(A+B)(x) \overset{\substack{\text{wie in (f)} \\ \downarrow}}}{=} ev(A)(x) + \overset{\substack{\text{in } \mathbb{R}}}{\leftarrow} ev(B)(x)$$

$$\overset{\substack{\text{Def. von } + \\ \text{auf } \text{Abb}(\mathbb{R}, \mathbb{R})}}{\downarrow} = \underset{\substack{\uparrow \text{ in } \text{Abb}(\mathbb{R}, \mathbb{R})}}{(ev(A) + ev(B))}(x)$$

- $ev(r \cdot A) = r \cdot ev(A)$, denn für jedes $x \in \mathbb{R}$ gilt:

$$ev(r \cdot A)(x) \overset{\substack{\text{wie in (f)} \\ \downarrow}}}{=} r \cdot \overset{\substack{\text{in } \mathbb{R}}}{\leftarrow} ev(A)(x)$$

$$\overset{\substack{\text{Def. von} \\ \text{Skalarmultiplikation} \\ \text{auf } \text{Abb}(\mathbb{R}, \mathbb{R})}}{\downarrow} = \underset{\substack{\uparrow \text{ in } \text{Abb}(\mathbb{R}, \mathbb{R})}}{(r \cdot ev(A))}(x)$$

3 | Strukturwandel ★

Wie viele Abbildungen $\mathbb{Z}/3\mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z}$ gibt es? Wie viele Gruppenhomomorphismen? Wie viele Ringhomomorphismen?

Abbildungen:

Für jedes der drei Elemente von $\mathbb{Z}/3\mathbb{Z}$ gibt es 6 verschiedene Werte, die angenommen werden können. Also gibt es genau 6^3 versch.

Abb. $\mathbb{Z}/3\mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z}$.

Gruppenhomos:

Es gibt mindestens drei Gruppenhomos. $\mathbb{Z}/3\mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z}$:

$$\begin{aligned} \mathbb{Z}/3\mathbb{Z} &\rightarrow \mathbb{Z}/6\mathbb{Z} \\ [n] &\mapsto [0] \end{aligned}$$

$$\begin{aligned} \mathbb{Z}/3\mathbb{Z} &\rightarrow \mathbb{Z}/6\mathbb{Z} \\ [n] &\mapsto [2n] \end{aligned}$$

$$\begin{aligned} \mathbb{Z}/3\mathbb{Z} &\rightarrow \mathbb{Z}/6\mathbb{Z} \\ [n] &\mapsto [4n] \end{aligned}$$

Andererseits ist jeder Gruppenhomos. $f: \mathbb{Z}/3\mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z}$ eindeutig festgelegt durch $f([1])$, denn

$$f([0]) = [0]$$

$$f([2]) = f([1] + [1]) = f([1]) + f([1])$$

Für $f([1])$ muss gelten:

$$3 \cdot f([1]) = [0],$$

$$\text{denn } 3 \cdot f([1]) = f([1]) + f([1]) + f([1])$$

$$= f([1] + [1] + [1]) = f([0]) = [0]$$

Es gibt nur drei Elemente $x \in \mathbb{Z}/6\mathbb{Z}$ mit $3 \cdot x = 0$ (nämlich $[0], [2], [4]$). Also gibt es genau 3 Gruppenhomomorphismen.

Ringhomomorphismen:

Es gibt keinen Ringhomo, denn jeder Ringhomo f ist insbes. ein Gruppenhomo. und erfüllt ferner $f([1]) = [1]$. Aber keiner der oben gefundenen Gruppenhomo. hat diese zusätzliche Eigenschaft.

4 | Flachwurzler ★

Welche Nullstellen hat das Polynom $X^3 - 3X^2 + 2X$ über $\mathbb{Z}/12\mathbb{Z}$?

Welche Nullstellen hat es über $\mathbb{Z}/101\mathbb{Z}$?

Nullstellen über $\mathbb{Z}/12\mathbb{Z}$:

Direktes Nachrechnen liefert Nullstellen

$[0], [1], [2], [4], [5], [6], [8], [9], [10]$

$$\begin{aligned} f([3]) &= [3]^3 - 3[3]^2 + 2[3] \\ &= [3] \cdot [9] - 3 \cdot [9] + [6] \\ &= [3] \cdot [-3] - 3 \cdot [-3] + [6] \\ &= \cancel{[-9]} - \cancel{[-9]} + [6] \\ &= [6] \neq [0] \end{aligned}$$

$$\begin{aligned} f([7]) &= [7]^3 - 3 \cdot [7]^2 + 2 \cdot [7] \\ &= [-5]^3 - 3 \cdot [-5]^2 + 2 \cdot [-5] \\ &= [-5] \cdot [25] - 3 \cdot [25] + 2 \cdot [-5] \\ &= [-5] \cdot [1] - 3 \cdot [1] + 2 \cdot [-5] \\ &= [-18] \\ &= [6] \neq [0] \end{aligned}$$

$$\begin{aligned} f([11]) &= f([-1]) \\ &= [-1]^3 - 3 \cdot [-1]^2 + 2 \cdot [-1] \\ &= [-1 - 3 - 2] \\ &= [6] \neq [0] \end{aligned}$$

Nullstellen über $\mathbb{Z}/101\mathbb{Z}$:

101 ist eine Primzahl, also ist $\mathbb{Z}/101\mathbb{Z}$

ein Körper, also hat das Polynom

höchstens 3 verschiedene Nullstellen

(Korollar 3.20).

↑
Grad des Polynoms

Wir raten z.B. $[0]$, $[1]$ & $[2]$ und rechnen nach:

$$[0]^3 - 3[0]^2 + 2[0] = [0] \quad \checkmark$$

$$[1]^3 - 3[1]^2 + 2[1] = [0] \quad \checkmark$$

$$[2]^3 - 3[2]^2 + 2[2] = [8 - 3 \cdot 4 + 4] = [0] \quad \checkmark$$

Also gibt es genau 3 Nullstellen.

