# Einführung in die Algebra

## Blatt 8

Jendrik Stelzner

12. Dezember 2013

## Aufgabe 8.1.

### (i)

Da $rs \cdot 1 = rs \cdot 1$ für alle $(r, s) \in R \times S$ mit $1 \in S$ ist $\sim$ reflexiv. Die Symmetrie von $\sim$ ergibt sich direkt aus der Symmetrie der Gleichheit. Für $(r, s), (r', s'), (r'', s'') \in R \times S$ mit $(r, s) \sim (r', s') \sim (r'', s'')$ gibt es $t, \tilde{t} \in S$ mit

$$rs't = r'st \text{ und} \tag{1}$$
$$r's''\tilde{t} = r''s'\tilde{t}. \tag{2}$$

Wegen der Abgeschlossenheit von $S$ unter Multiplikation ist auch $s't\tilde{t} \in S$, und wegen der Kommutativität von $R$ daher

$$rs''s't\tilde{t} \underset{(1)}{=} r's''st\tilde{t} \underset{(2)}{=} r''s'st\tilde{t} = r''ss't\tilde{t}.$$

Also ist $(r, s'') \sim (r'', s)$ und $\sim$ daher transitiv.

### (ii)

Aus der Notation der Restklassen und der Definition von $\sim$ folgt direkt, dass für alle $(r, s), (r', s') \in R \times S$

$$\frac{r}{s} = \frac{r'}{s'} \Leftrightarrow \text{ es gibt } t \in S \text{ mit } rs't = r'st. \tag{3}$$

Zunächst die Wohldefiniertheit: Seien $(r, s), (\tilde{r}, \tilde{s}) \in R \times S$ mit $(r, s) \sim (\tilde{r}, \tilde{s})$. Dann gibt es $t \in S$ mit $r\tilde{s}t = \tilde{r}st$. Wegen der Kommutativität von $R$ ist daher für alle $(r', s') \in R \times S$

$$(rs' + r's)\tilde{s}s't = rs'\tilde{s}s't + r's\tilde{s}s't = \tilde{r}s'ss't + r's\tilde{s}s't = (\tilde{r}s', r'\tilde{s})ss't,$$

und

$$rr'\tilde{s}s't = \tilde{r}r'ss't.$$

Da die Ausdrücke

$$\frac{rs' + r's}{ss'} \text{ und } \frac{rr'}{ss'}$$

wegen der Kommutativität von $R$ symmetrisch in $(r,s)$ und $(r',s')$ sind folgt damit wegen (3) die Wohldefiniertheit.
Es ist klar, dass $R[S^{-1}]$ unter Addition und Multiplikation abgeschlossen ist. Die Addition ist assoziativ und kommutativ, da wegen der Kommutatvität von $R$ für alle $\frac{r}{s}, \frac{r'}{s'}, \frac{r''}{s''} \in R[S^{-1}]$

$$\begin{aligned}\frac{r}{s}+\left(\frac{r'}{s'}+\frac{r''}{s''}\right) &= \frac{r}{s}+\frac{r's''+r''s'}{s's''} = \frac{rs's''+r'ss''+r''ss'}{ss's''}\\ &= \frac{rs'+r's}{ss'}+\frac{r''}{s''} = \left(\frac{r}{s}+\frac{r'}{s'}\right)+\frac{r''}{s''},\end{aligned}$$

sowie

$$\frac{r}{s}+\frac{r'}{s'} = \frac{rs'+r's}{ss'} = \frac{r's+rs'}{s's} = \frac{r'}{s'}+\frac{r}{s}.$$

Das Element $\frac{0}{1} \in R[S^{-1}]$ ist bezüglich der Addition neutral, da für alle $\frac{r}{s} \in R[S^{-1}]$

$$\frac{r}{s}+\frac{0}{1} = \frac{r\cdot 1+s\cdot 0}{s\cdot 1} = \frac{r}{s},$$

und $\frac{r}{s} \in R[S^{-1}]$ hat als additives Inverses $\frac{-r}{s}$, da

$$\frac{r}{s}+\frac{-r}{s} = \frac{rs-rs}{s^2} = \frac{0}{s^2} = \frac{0}{1},$$

denn aus der Definition von $\sim$ folgt offenbar direkt, dass $\frac{0}{s} = \frac{0}{1}$ für alle $s \in S$, und wegen der Abgeschlossenheit von $S$ bezüglich der Multiplikation ist $s^2 \in S$. Also ist $R[S^{-1}]$ bezüglich der Addition eine abelsche Gruppe.
Da Multiplikation ist assoziativ und kommutativ, da für alle $\frac{r}{s}, \frac{r'}{s'}, \frac{r''}{s''} \in R[S^{-1}]$

$$\frac{r}{s}\left(\frac{r'}{s'}\frac{r''}{s''}\right) = \frac{r}{s}\frac{r'r''}{s's''} = \frac{rr'r''}{ss's''} = \frac{rr'}{ss'}\frac{r''}{s''} = \left(\frac{r}{s}\frac{r'}{s'}\right)\frac{r''}{s''},$$

und wegen der Kommutativität von $R$

$$\frac{r}{s}\frac{r'}{s'} = \frac{rr'}{ss'} = \frac{r'r}{s's} = \frac{r'}{s'}\frac{r}{s}.$$

Das Element $\frac{1}{1} \in R[S^{-1}]$ ist das multiplikativ Neutrale in $R[S^{-1}]$, da für alle $\frac{r}{s} \in R[S^{-1}]$

$$\frac{1}{1}\frac{r}{s} = \frac{r}{s}\frac{1}{1} = \frac{r\cdot 1}{s\cdot 1} = \frac{r}{s}.$$

Dies zeigt, dass $R[S^{-1}]$ bezüglich der Multiplikation ein abelsches Monoid ist.
Zum Nachweis des Distributivgesetzes bemerken wir zunächst:

**Bemerkung 1**. *Für alle $\frac{r}{s} \in R[S^{-1}]$ und $t \in S$ gilt nach* (3) *die Kürzungsregel*

$$\frac{rt}{st} = \frac{r}{s},$$

*denn wegen der Kommutativität von $R$ ist $rts\cdot 1 = rst\cdot 1$ mit $1 \in S$. Insbesondere gilt für alle $s \in S$*

$$\frac{s}{1}\cdot\frac{1}{s} = \frac{s}{s} = \frac{1}{1}.$$

Mit der obigen Bemerkung erhalten wir, dass für alle $\frac{r}{s}, \frac{r'}{s'}, \frac{r''}{s''} \in R[S^{-1}]$

$$\begin{aligned}\frac{r}{s}\left(\frac{r'}{s'}+\frac{r''}{s''}\right) &= \frac{r}{s}\frac{r's''+r''s'}{s's''} = \frac{rr's''+rr''s'}{ss's''} \\ &= \frac{rr'ss'+rr''ss'}{s^2s's''} = \frac{rr'}{ss'}+\frac{rr''}{ss''} = \frac{r}{s}\frac{r'}{s'}+\frac{r}{s}\frac{r''}{s''}.\end{aligned}$$

Dies zeigt, dass $R[S^{-1}]$ ein kommutativer Ring (mit Einselement) ist.

## (iii)

Da für alle $r, r' \in R$

$$\varphi(r+r') = \frac{r'+r}{1} = \frac{r\cdot 1 + r'\cdot 1}{1^2} = \frac{r}{1}+\frac{r'}{1} = \varphi(r)+\varphi(r'),$$

und

$$\varphi(rr') = \frac{rr'}{1} = \frac{rr'}{1^2} = \frac{r}{1}\frac{r'}{1} = \varphi(r)\varphi(r')$$

sowie

$$\varphi(1_R) = \frac{1}{1} = 1_{R[S^{-1}]}$$

ist $\varphi$ ein Ringhomomorphismus. Aus Bemerkung 1 folgt, dass $\varphi(S) \subseteq (R[S^{-1}])^*$.
Wir bemerken auch direkt, dass $\varphi$ nicht zwangsweise injektiv ist: Ist $R \neq 0$ und $0 \in S$, etwa $S = R$ oder $S = \{0,1\}$, so ist offenbar $R[S^{-1}] \cong 0$, also $\varphi = 0$ und wegen $R \neq 0$ damit nicht injektiv.
Für einen Homomorphismus $\psi_S : R[S^{-1}] \to R'$ mit $\psi = \psi_S \circ \varphi$ muss für alle $r \in R$ und $s \in S$

$$\psi_S\left(\frac{r}{1}\right) = \psi_S(\varphi(r)) = \psi(r)$$

und daher

$$\psi_S\left(\frac{1}{s}\right) = \psi_S\left(\left(\frac{s}{1}\right)^{-1}\right) = \psi_S\left(\frac{s}{1}\right)^{-1} = \psi_S(s)^{-1},$$

da $\psi_S$ durch Einschränkung einen Gruppenhomomorphismus von $(R[S^{-1}])^*$ nach $(R')^*$ induziert. Also ist $\psi_S$ durch

$$\psi_S\left(\frac{r}{s}\right) = \psi_S\left(\frac{r}{1}\frac{1}{s}\right) = \psi_S\left(\frac{r}{1}\right)\psi_S\left(\frac{1}{s}\right) = \psi(r)\psi(s)^{-1}$$

für alle $\frac{r}{s} \in R[S^{-1}]$ eindeutig bestimmt. Definiert man $\psi_S$ auf diese Art, so handelt es sich bei $\psi_S$ um einen Ringhomomorphismus, denn für alle $\frac{r}{s}, \frac{r'}{s'} \in R[S^{-}1]$ ist

$$\begin{aligned}\psi_S\left(\frac{r}{s}+\frac{r'}{s'}\right) &= \psi_S\left(\frac{rs'+r's}{ss'}\right) = \psi(rs'+r's)\psi(ss)^{-1} \\ &= \left(\psi(r)\psi(s')+\psi(r')\psi(s)\right)\psi(s)^{-1}\psi(s')^{-1}\psi \\ &= \psi(r)\psi(s)^{-1}+\psi(r')\psi(s')^{-1} = \psi_S\left(\frac{r}{s}\right)+\psi_S\left(\frac{r'}{s'}\right),\end{aligned}$$

sowie

$$\begin{aligned}\psi_S\left(\frac{r}{s}\frac{r'}{s'}\right) &= \psi_S\left(\frac{rr'}{ss'}\right) = \psi(rr')\psi(ss')^{-1} \\ &= \psi(r)\psi(r')\psi(s)^{-1}\psi(s')^{-1} \\ &= \psi(r)\psi(s)^{-1}\psi(r')\psi(s')^{-1} = \psi_S\left(\frac{r}{s}\right)\psi_S\left(\frac{r'}{s'}\right),\end{aligned}$$

und inbesondere

$$\psi_S\left(1_{R[S^{-1}]}\right) = \psi_S\left(\frac{1}{1}\right) = \psi(1)\psi(1)^{-1} = 1_{R'}.$$

# Aufgabe 8.2.

Da ich diese Aufgabe sehr hässlich aufzuschreiben finde, gibt es hier nur kurze Skizze eines Beweises:
Zunächst bemerkt man, dass ein Unterring $R \subseteq \mathbb{Q}$ von der Menge

$$T_R = \left\{\frac{1}{p} \in R : p \in P\right\}$$

erzeugt wird. Dadurch ergibt sich direkt, dass jeder Unterring von $\mathbb{Q}$ eindeutig dadurch festgelegt ist, welche Primzahlen in ihm invertierbar sind. Für jede Teilmenge $T \subseteq P$ ist die Lokalisierung $\mathbb{Z}[S(T)^{-1}]$ genau die Erweiterung von $\mathbb{Z}$, in der alle Elemente von $T^c = P \setminus T$ invertierbar sind, und alle Elemente von $T$ nicht. Das Bild von $\psi_{S(T)}$ entspricht daher dem von

$$(T^c)^{-1} = \left\{\frac{1}{p} : p \in T^c\right\}$$

erzeugten Unterring von $\mathbb{Q}$. Die Injektivität der Abbildung ergibt sich direkt aus der Nullteilerfreiheitvon $\mathbb{Z}$ und der Definition von $\psi_{S(T)}$. Die Surjektivität ergibt sich direkt daraus, dass man für einen Unterring $R$ von $\mathbb{Q}$ geneau $\mathbb{Z}[S(T_R^c)^{-1}]$ wählen kann.

# Aufgabe 8.3.

**Bemerkung 2**. *Sei $R$ ein kommutativer Ring. Dann ist $R$ genau dann noethersch, wenn jedes Ideal von $R$ endlich erzeugt ist.*

*Beweis.* Angenommen $R$ ist noethersch. Sei $I \subseteq R$ ein Ideal. Wir konstruieren eine wachsende Folge $I_0 \subseteq I_1 \subseteq \ldots$ von Idealen von $R$, mit $I_n \subseteq I$ für alle $n \in \mathbb{N}$, rekursiv wie folgt: Wir setzen $I_0 := 0$. Für $n \geq 1$ setzen wir $I_n := I_{n-1} + (a_n)$, falls es ein $a_n \in I \setminus I_{n-1}$ gibt, und sonst $I_n := I_{n-1}$. Da $R$ noethersch ist stabilisiert sich die Folge $(I_n)_{n\in\mathbb{N}}$, d.h. es gibt ein $N \in \mathbb{N}$ mit $I_{n+1} = I_n$ für alle $n \geq N$. Insbesondere ist $I_{N+1} = I_N$, nach Definition und von $I_{N+1}$ und $I_N \subseteq I$ also $I = I_N$. Daher ist

$$I = I_N = (a_1) + \ldots + (a_N) = (a_1, \ldots, a_N)$$

endlich erzeugt.

Angenommen, jedes Ideal in von $R$. Für eine wachsende Folge $I_0 \subseteq I_1 \subseteq \dots$ von Idealen von $R$ setzen wir $I = \bigcup_{n\in\mathbb{N}} I_n = \sum_{n\in\mathbb{N}} I_n$. $I$ ist als Ideal von $R$ endlich erzeugt, es gibt also $a_1, \dots, a_m \in \mathbb{R}$ mit $I = (a_1, \dots, a_m)$. Nach Definition von $I$ gibt es ein $N \in \mathbb{N}$ mit $a_1, \dots, a_m \in I_N$. Also ist $I = I_N$, und damit $I_n = I_{n+1}$ für alle $n \geq N$. □

**Bemerkung 3**. *Faktorringe kommutativer, noetherscher Ringe sind noethersch.*

*Beweis.* Sei $R$ ein kommutativer, noetherscher Ring und $I \subseteq R$ ein Ideal. Die kanonische Projektion $\pi : R \twoheadrightarrow R/I$ induziert eine Bijektion zwischen den Idealen von $R/I$ und den Idealen von $R$, die $I$ beinhalten. Jede wachsende Folge $J_0 \subseteq J_1 \subseteq \dots$ von Idealen von $R/I$ entspricht daher einer wachsenden Folge $I_0 \subseteq I_1 \subseteq \dots$ von Idealen von $R$ mit $I \subseteq I_i$ für alle $i \in \mathbb{N}$. Da $R$ noethersch ist stabilisiert sich die Folge $(I_n)_{n\in\mathbb{N}}$ in $R$, also auch die Folge $(J_n)_{n\in\mathbb{N}}$ in $R/I$. Also ist $R/I$ noethersch. □

Wir zeigen nun, dass auch Lokalisierungen kommutativer, noetherscher Ringe wieder noethersch sind: Es sei $R$ ein kommutativer, noetherscher Ring und $S \subseteq R$ ein Untermonoid bezüglich der Multiplikation. Es sei $I \subseteq R[S^{-1}]$ ein Ideal. Wir setzen

$$J := \left\{ \frac{r}{1} \in I : r \in R \right\}.$$

Es ist $(J)_{R[S^{-1}]} = I$, wobei $(J)_{R[S^{-1}]}$ das von $J$ in $R[S^{-1}]$ erzeugte Ideal bezeichnet. Es ist klar, dass $(J)_{R[S^{-1}]} \subseteq I$. Andererseits ist für alle $\frac{r}{s} \in I$ auch $\frac{s}{1}\frac{r}{s} = \frac{rs}{s} = \frac{r}{1} \in I$, also $\frac{r}{1} \in J$, und daher auch $\frac{r}{s} = \frac{1}{s}\frac{r}{1} \in (J)_{R[S^{-1}]}$.
Es ist $J \subseteq \operatorname{Im}\varphi$, wobei $\varphi : R \to R[S^{-1}], r \mapsto \frac{r}{1}$. Da $R$ noethersch ist, ist es nach Bemerkung 3 auch $\operatorname{Im}\varphi \cong R/\operatorname{Ker}\varphi$. Es gibt also $a_1, \dots, a_n \in \operatorname{Im}\varphi$ mit $(J)_{\operatorname{Im}\varphi} = (a_1, \dots, a_n)_{\operatorname{Im}\varphi}$. Es ist daher

$$\begin{aligned} I = (J)_{R[S^{-1}]} &= ((J)_{\operatorname{Im}\varphi})_{R[S^{-1}]} \\ &= ((a_1, \dots, a_n)_{\operatorname{Im}\varphi})_{R[S^{-1}]} = (a_1, \dots, a_n)_{R[S^{-1}]}, \end{aligned}$$

also $I$ in $R[S^{-1}]$ endlich erzeugt. Aus Bemerkung 2 folgt, dass $R[S^{-1}]$ noethersch ist.

# Aufgabe 8.4.

Ich werde im Folgenden Summen der Form $f = \sum_{i,j\in\mathbb{N}} a_{ij} X_1^i X_2^j$ für $f \in \mathbb{Z}[X_1, X_2]$, bzw. $f \in \mathbb{Q}[X_1, X_2]$ nutzen, ohne jedes Mal explizit anzugeben, dass fast alle $a_{ij}$ gleich null sind.

## (i)

$\mathbb{Z}[X_1, X_2]$

Das Ideal ist in $\mathbb{Z}[X_1, X_2]$ nicht maximal, da

$$(X_1, X_2, 2) = \left\{ \sum_{i,j\in\mathbb{N}} a_{ij} X_1^i X_2^j : a_{0,0} \text{ ist gerade} \right\}$$

ein größeres echtes Ideal von $\mathbb{Z}[X_1, X_2]$ ist. Es ist jedoch ein Primideal: Für $f, g \notin (X_1, X_2)$ mit $f = \sum_{i,j\in\mathbb{N}} a_{ij} X_1^i X_2^j$ und $g = \sum_{i,j\in\mathbb{N}} b_{ij} X_1^i X_2^j$ ist $f, g \neq 0$ und $a_{0,0}, b_{0,0} = 0$. Da $\mathbb{Z}[X_1, X_2]$ ein Integritätsring ist, ist $0 \neq fg = \sum_{i,j\in\mathbb{N}} c_{ij} X_1^i X_2^j$, und wegen $c_{0,0} = a_{0,0} b_{0,0} = 0$ also $fg \notin (X_1, X_2)$.

$\mathbb{Q}[X_1, X_2]$

Das Ideal ist maximal in $\mathbb{Q}[X_1, X_2]$. Für $f \notin (X_1, X_2)$ muss $f = \sum_{i,j\in\mathbb{N}} a_{ij} X_1^i X_2^j$ mit $a_{0,0} \neq 0$. Dann ist aber $a_{0,0} \in (X_1, X_2, f)$, also, da $a_{0,0} \in \mathbb{Q}^* = (\mathbb{Q}[X_1, X_2])^*$, bereits $(X_1, X_2, f) = \mathbb{Q}[X_1, X_2]$. Als maximales Ideal ist $(X_1, X_2)$ insbesondere ein Primideal.

## (ii)

$\mathbb{Z}[X_1, X_2]$

Das Ideal ist nicht maximal in $\mathbb{Z}[X_1, X_2]$, da $(X_1 + X_2, X_1) = (X_1, X_2)$ ein größeres echtes Ideal von $\mathbb{Z}[X_1, X_2]$ ist. $X_1 + X_2$ ist irreduzibel in $\mathbb{Z}[X_1, X_2]$: Für $f, g \in \mathbb{Z}[X_1, X_2]$ mit $fg = X_1 + X_2$ muss $1 = \deg(X_1 + X_2) = \deg(f) + \deg(g)$, also o.B.d.A. $\deg(f) = 0$ und $\deg(g) = 1$. Also ist $f = c \in \mathbb{Z} \setminus \{0\}$ und $g = \frac{1}{c}X_1 + \frac{1}{c}X_2$. Da $\frac{1}{c} \in \mathbb{Z}$ muss $c = 1$ oder $c = -1$, also $c \in \mathbb{Z}^* = (\mathbb{Z}[X_1, X_2])^*$. Da $\mathbb{Z}[X_1, X_2]$ nach dem Satz von Gauß faktoriell ist, ist $X_1 + X_2$ daher prim in $\mathbb{Z}[X_1, X_2]$, also $(X_1 + X_2)$ ein Primideal in $\mathbb{Z}[X_1, X_2]$.

$\mathbb{Q}[X_1, X_2]$

Es ergibt sich analog zur Argumentation für $\mathbb{Z}[X_1, X_2]$, dass das Ideal prim aber nicht maximal in $\mathbb{Q}[X_1, X_2]$ ist. Dabei ergibt sich $f \in (\mathbb{Q}[X_1, X_2])^*$ bereits durch $\deg(f) = 0$.

## (iii)

$\mathbb{Z}[X_1, X_2]$

Das Ideal ist maximal, und damit auch prim, in $\mathbb{Z}[X_1, X_2]$: Für $f \notin (X_1, X_2, 2)$ mit $f = \sum_{i,j\in\mathbb{N}} a_{i,j} X_1^i X_2^j$ muss $a_{0,0}$ ungerade sein. Es ist daher $f + 1 \in (X_1, X_2, 2)$, und somit $1 \in (X_1, X_2, 2, f)$, also bereits $(X_1, X_2, 2, f) = \mathbb{Z}[X_1, X_2]$.

$\mathbb{Q}[X_1, X_2]$

Da $(X_1, X_2, 2) \ni 2 \in \mathbb{Q}^* = (\mathbb{Q}[X_1, X_2])^*$ ist bereits $(X_1, X_2, 2) = \mathbb{Q}[X_1, X_2]$, also das Ideal weder prim noch maximal in $\mathbb{Q}[X_1, X_2]$.

## (iv)

Es sei im Folgenden $R = \mathbb{Z}$ oder $R = \mathbb{Q}$, der Beweis läuft unabhängig von der Wahl des Ringes. Es ist

$$A := (X_1 + X_2^2, X_1^2 + X_2)_{R[X_1,X_2]}$$

kein Primideal, und damit auch kein maximales Ideal, von $R[X_1, X_2]$: Wir nehmen an, dass $A$ prim ist. Es ist

$$X_1^2(X_1 + X_2^2) = X_1^3 + X_1^2 X_2^2 \in A \text{ und } X_2^2(X_1^2 + X_2) = X_1^2 X_2^2 + X_2^3 \in A,$$

also auch $X_1^3 - X_2^3 \in A$. Da

$$X_1^3 - X_2^3 = (X_1^2 + X_1 X_2 + X_2^2)(X_1 - X_2)$$

muss nach Annahme $X_1^2 + X_1X_2 + X_2^2 \in A$ oder $X_1 - X_2 \in A$. Da $X_1 + X_2^2$ und $X_1^2 + X_2$ bei $(-1,-1)$ eine Nullstellle haben, muss $f(-1,-1) = 0$ für alle $f \in A$. Da dies für $X_1^2 + X_1X_2 + X_2^2$ nicht der Fall ist, muss also $X_1 - X_2 \in A$.
Es gibt also $f, g \in R[X_1, X_2]$ mit $f \cdot (X_1^2 + X_2) + g \cdot (X_1 + X_2^2) = X_1 - X_2$. Durch den Einsetzhomomorphismus ergibt sich, dass für alle $x \in R$ mit $x > 0$

$$0 = f(x)(x + x^2) + g(x)(x^2 + x) = (f + g)(x)\underbrace{(x + x^2)}_{\neq 0}.$$

Es muss also $f + g$ unendlich viele Nullstellen haben, also $f + g = 0$ und daher $f = -g$. Also ist

$$f \cdot (X_1^2 + X_2 - X_1 - X_2^2) = X_1 - X_2.$$

Insbesondere ist, da $R$ ein Integritätsring ist,

$$\deg(f)\deg(X_1^2 + X_2 - X_1 - X_2^2) = \deg(X_1 - X_2),$$

also $2\deg(f) = 1$, was offenbar nicht möglich ist. Also ist $A$ nicht prim.

# Aufgabe 8.5.

## (i)

Gebe es $f, g \in \mathbb{Q}[X]$ mit $f, g \notin (\mathbb{Q}[X])^* = \mathbb{Q}^*$ und $fg = X^3 - 2$, so muss $\deg f = 1$ oder $\deg g = 1$, da dann $1 \leq \deg f, \deg g \leq 3$ und $\deg f + \deg g = 3$. Also müsste $X^3 - 2$ dann eine rationale Nullstelle besitzen. Die einzige reelle Nullstelle des Polynomes ist jedoch $\sqrt[3]{2} \notin \mathbb{Q}$, weshalb dies nicht möglich ist.

## (ii)

Betrachten wir die Primzahl $p = 3 \in \mathbb{Z}$, so ergibt sich durch Reduktion der Koeffizienten bezüglich $p$ aus $X^3 + 39X^2 - 4X + 8 \in \mathbb{Z}[X]$ das Polynom

$$X^3 - X + 2 \in \mathbb{F}_3[X].$$

Dieses hat keine Nullstellen in $\mathbb{F}_3$, es ergibt sich also analog zur obigen Argumentation, dass es irreduzibel (in $\mathbb{F}_3[X]$) ist. Nach dem Reduktionskriterium ist daher auch $X^3 + 39X^2 - 4X + 8 \in \mathbb{Q}[X]$ irreduzibel.

## (iii)

Es ist bekannt, dass $f = X^6 + X^3 + 1 \in \mathbb{Z}[X]$ genau dann irreduzibel ist, wenn $f(X + 1)$ irreduzibel ist. Da

$$\begin{aligned} f(X + 1) &= (X + 1)^6 + (X + 1)^3 + 1 \\ &= X^6 + 6X^5 + 15X^4 + 21X^3 + 18X + 9X + 3 \end{aligned}$$

ergibt sich dies aus dem Eisensteinkriterium, indem man die Primzahl $p = 3$ betrachtet. ($f(X + 1)$ ist als normiertes Polynom offenbar primitiv.) Inbesondere ergibt sich damit auch, dass $f$ irreduzibel in $\mathbb{Q}[X]$ ist.

## (iv)

Für die Primzahl $7 \in \mathbb{Z}$ ergibt sich durch Reduktion der Koeffizienten aus $X^7+21X^5+35X^2+34X-8 \in \mathbb{Z}[X]$ das Polynom

$$X^7 - X - 1 \in \mathbb{F}_7[X].$$

Wie die folgende Bemerkung zeigen wird, ist dieses irreduzibel in $\mathbb{F}_7[X]$, und daher das ursprüngliche Polynom nach dem Reduktionskriterium in $\mathbb{Q}[X]$ irreduzibel.

**Bemerkung 4**. *Sei $p > 0$ eine Primzahl. Dann ist das Polynom $f = X^p - X - 1 \in \mathbb{F}_p[X]$ irreduzibel.*

*Beweis.* Wir nehmen an, dass $f$ reduzibel in $\mathbb{F}_p[X]$ ist. Wir wählen als Repräsentantensystem $P$ der Primelemente von $\mathbb{F}_p[X]$ die normierten Primelemente. Da $\mathbb{F}_p$ ein Körper ist, ist $\mathbb{F}_p[X]$ ein faktorieller Ring, es gibt also eindeutig bestimmte $\varepsilon \in \mathbb{F}_p$ und $g_1, \dots, g_n \in P$, $n \geq 2$, mit

$$f = \varepsilon g_1 \cdots g_n. \tag{4}$$

Da $f$ und $g_1, \dots, g_n$ normiert sind, ist dabei $\varepsilon = 1$. Wir bemerken, dass $f$ bezüglich der Abbildung

$$\tau : \mathbb{F}_p[X] \to \mathbb{F}_p[X], h \mapsto h(X+1)$$

invariant ist, da

$$\tau(f) = (X+1)^p - (X+1) - 1 = \left(\sum_{k=0}^{p} \binom{p}{k} X^k\right) - X = X^p - X - 1 = f.$$

Dabei setzen wir

$$\binom{p}{p} = 1.$$

Es ist klar, dass $\tau$ ein Ringautomorphismus ist. Insbesondere ist

$$f = \tau(f) = \tau(g_1 \cdots g_n) = \tau(g_1) \cdots \tau(g_n).$$

Da die Darstellung (4) bis auf Assoziiertheit und Reihenfolge der Faktoren eindeutig ist, gibt es daher für alle $i = 1, \dots, n$ je $\varepsilon_i \in \mathbb{F}_p$ und $\sigma \in \mathfrak{S}_n$ mit

$$\tau(g_i) = \varepsilon_i g_{\sigma(i)} \text{ für alle } i = 1, \dots, n.$$

Da $(X+p)^n = X^n$ für alle $n \in \mathbb{N}$ ist $\tau^p = \mathrm{id}$. Es ist daher insbesondere $\sigma^p = 1$. Folglich ist $\operatorname{ord}\sigma \mid p$, also $\operatorname{ord}\sigma = 1$ oder $\operatorname{ord}\sigma = p$.
Ist $\operatorname{ord}\sigma = p$, so muss $\sigma$ in Zykelschreibweise einen Zykel der Ordnung $p$ haben, also mindestens $p$ Element miteinander kommutieren, d.h. $n \geq p$. Da $\deg(g_i) \geq 1$ für alle $i = 1, \dots, n$ und $\sum_{i=1}^{n} \deg(g_i) = \deg(X^p - X - 1) = p$ muss $n = p$ und $\deg(g_i) = 1$ für alle $1 = 1, \dots, n$. Folglich besitzt $f$ mindestens eine Nullstelle; dies ist jedoch nicht der Fall, da $f(x) = -1 \neq 0$ für alle $x \in \mathbb{F}_p$. Ist $\operatorname{ord}\sigma = 1$, so sind die $g_i$ bis auf Assoziiertheit invariant unter $\tau$. Da dann

$$\tau^p(g_i) = \varepsilon_i^p g_i = 1 g_i$$

muss $\varepsilon_i^p = 1$, nach dem kleinen Fermatschen Satz also $\varepsilon = 1$ und damit $\tau(g_i) = g_i$ für $i = 1, \dots, n$. Da $g_1$ invariant unter $\tau$ ist, ist

$$g_1(x) = g_1(0) \text{ für alle } x \in \mathbb{F}_p[X].$$

Folglich ist $g_1 - g_1(0) = 0$. Da jedoch $\deg(g_1 - g_1(0)) = \deg(g_1)$ und $0 < \deg(g_1) < \deg(X^p - X - 1) = p$ ist dies ein Widerspruch dazu, dass $g_1 - g_1(0)$ höchstens $\deg(g_1 - g_1(0))$ viele Nullstellen haben kann. $\square$