

# Übungen zu Einführung in die Algebra

Jendrik Stelzner

12. Dezember 2016

## Inhaltsverzeichnis

1	Gruppentheorie	2
2	Ringtheorie	6
3	Modultheorie	18
4	Körpertheorie	21

# 1 Gruppentheorie

## Übung 1. Ein Kriterium für maximale Untergruppen

Es sei  $G$  eine Gruppe und  $H \subseteq G$  eine Untergruppe, so dass  $[G : H]$  endlich und prim ist. Zeigen Sie, dass  $H$  eine maximale echte Untergruppe von  $G$  ist. Entscheiden Sie, ob  $H$  notwendigerweise normal in  $G$  ist.

### Lösung 1.

Es sei  $p := [G : H]$ . Da  $p$  eine Primzahl ist gilt insbesondere  $p \neq 1$ , weshalb  $H$  eine echte Untergruppe von  $G$  ist. Ist  $K \subsetneq G$  eine echte Untergruppe von  $G$  mit  $H \subseteq K$ , so gilt wegen der Multiplikativität des Index, dass

$$p = [G : H] = [G : K][K : H].$$

Da  $p$  eine Primzahl ist, gilt entweder  $[G : K] = p$  und  $[K : H] = 1$ , oder  $[G : K] = 1$  und  $[K : H] = p$ . Es gilt  $[G : K] > 1$ , da  $K$  eine echte Untergruppe von  $G$  ist, und somit  $[K : H] = 1$ . Also ist  $K = H$ , und somit  $H$  eine maximale echte Untergruppe.

$H$  ist nicht notwendigerweise normal in  $G$ : Für  $G = S_3$  und  $H = \langle (1\ 2) \rangle = \{\text{id}, (1\ 2)\}$  ist  $H$  zwar nicht normal in  $G$ , aber  $[G : H] = |G|/|H| = 6/2 = 3$  ist prim.

## Übung 2. Multiple Choice I

Entscheiden Sie, ob die folgenden Aussagen allgemein gültig sind, und geben sie gegebenenfalls ein Gegenbeispiel an.

1. Ist  $G$  eine Gruppe und  $N \subseteq G$  eine normale Untergruppe, so gilt  $G \cong (G/N) \times N$ .
2. Ist  $G$  eine endliche Gruppe, so dass  $G/N$  für normale Untergruppe  $N \subseteq G$  mit  $N \neq 1$  abelsch ist, so ist auch  $G$  abelsch.
3. Zwei Gruppen  $G_1$  und  $G_2$  sind genau dann isomorph, wenn  $G_1 \times H \cong G_2 \times H$  für jede Gruppe  $H$ .
4. Sind  $G_1$  und  $G_2$  zwei Gruppen, so ist jede Untergruppe von  $G_1 \times G_2$  von der Form  $H_1 \times H_2$  für Untergruppen  $H_1 \subseteq G_1$  und  $H_2 \subseteq G_2$ .
5. Sind  $G_1$  und  $G_2$  zwei Gruppen, so dass es Gruppenepimorphismen  $\phi: G_1 \rightarrow G_2$  und  $\psi: G_2 \rightarrow G_1$  gibt, so gilt  $G_1 \cong G_2$ .

### Lösung 2.

1. Die Aussage ist falsch: Es sei  $G = \mathbb{Z}$  und  $N = 2\mathbb{Z}$ . Dann ist

$$(G/N) \times N \cong (\mathbb{Z}/2\mathbb{Z}) \times (2\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}.$$

Es ist allerdings  $(\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z} \not\cong \mathbb{Z}$ , da  $(\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$  ein Element der Ordnung 2 enthält (nämlich  $(1, 0)$ ),  $\mathbb{Z}$  aber nicht.

2. Die Aussage ist falsch: Die einzigen nicht-trivialen normalen Untergruppe von  $S_3$  sind  $N = \langle (1\ 2\ 3) \rangle = \{\text{id}, (1\ 2\ 3), (1\ 3\ 2)\}$  und  $S_3$  selbst. Der Quotient  $S_3/N$  hat Ordnung 2, weshalb  $S_3/N \cong \mathbb{Z}/2\mathbb{Z}$  abelsch ist, und  $S_3/S_3 = 1$  ist ohnehin abelsch. Die Gruppe  $S_3$  selbst ist allerdings nicht abelsch.

Alternativ ist  $A_n$  für  $n \geq 5$  einfach, weshalb  $A_n$  der einzige nicht-triviale Normalteiler von  $A_n$  ist, aber  $A_4$  ist für  $n \geq 4$  nicht abelsch.

3. Die Aussage ist wahr: Gilt  $G_1 \cong G_2$ , so gibt es einen Isomorphismus  $\phi: G_1 \rightarrow G_2$ . Für jede Gruppe  $H$  ist dann  $\phi \times \text{id}_H: G_1 \times H \rightarrow G_2 \times H$  ein Isomorphismus, und somit  $G_1 \times H \cong G_2 \times H$ . Gilt andererseits  $G_1 \times H \cong G_2 \times H$  für jede Gruppe  $H$ , so gilt insbesondere  $G_1 \cong G_1 \times 1 \cong G_2 \times 1 \cong G_2$ .
4. Die Aussage ist falsch: Ist  $G \neq 1$  eine Gruppe und  $G_1 = G_2 = G$ , so ist die Diagonale  $\Delta = \{(g, g) \mid g \in G\}$  eine Untergruppe von  $G_1 \times G_2 = G \times G$ , die sich nicht als ein solches Produkt schreiben lässt.
5. Die Aussage ist falsch: Für die Gruppen

$$G_1 = \bigoplus_{n \in \mathbb{N}} \mathbb{Z} = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \dots$$

und

$$G_2 = \mathbb{Z}/2\mathbb{Z} \oplus \bigoplus_{n \in \mathbb{N}} \mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \dots$$

gibt es Gruppenepimorphismen

$$\phi: G_1 \rightarrow G_2, \quad (n_1, n_2, n_3, \dots) \mapsto (\overline{n_1}, n_2, n_3, \dots)$$

und

$$\psi: G_2 \rightarrow G_1, \quad (\overline{n_1}, n_2, n_3, \dots) \mapsto (n_2, n_3, \dots).$$

Es gilt aber  $G_1 \not\cong G_2$ , denn  $G_2$  enthält ein Element der Ordnung 2,  $G_1$  jedoch nicht.

### Übung 3.

Es seien  $G_1$  und  $G_2$  zwei Gruppen,  $N_1 \subseteq G_1$  und  $N_2 \subseteq G_2$  zwei normale Untergruppen. Geben Sie jeweils Beispiele für die folgenden Situationen:

1. Es gilt  $G_1 \cong G_2$  und  $N_1 \cong N_2$ , aber  $G_1/N_1 \not\cong G_2/N_2$ .
2. Es gilt  $G_1 \cong G_2$  und  $G_1/N_1 \cong G_2/N_2$ , aber  $N_1 \not\cong N_2$ .
3. Es gilt  $G_1/N_1 \cong G_2/N_2$  und  $N_1 \cong N_2$ , aber  $G_1 \not\cong G_2$ .

**Lösung 3.**

1. Es seien  $G_1 = G_2 = \bigoplus_{n \geq 0} \mathbb{Z}$ , sowie  $N_1 = \bigoplus_{n \geq 1} \mathbb{Z}$  und  $N_2 = \bigoplus_{n \geq 2} \mathbb{Z}$ . Dann gilt  $G_1 = G_2 \cong N_1 \cong N_2$  aber

$$G_1/N_1 \cong \mathbb{Z} \not\cong \mathbb{Z} \oplus \mathbb{Z} = G_2/N_2.$$

2. Es seien  $G_1 = G_2 = \bigoplus_{n \geq 0} \mathbb{Z}$  und

$$N_1 := \mathbb{Z} \oplus 0 \oplus 0 \oplus 0 \oplus \dots$$

und

$$N_2 := \mathbb{Z} \oplus \mathbb{Z} \oplus 0 \oplus 0 \oplus \dots$$

Dann gilt

$$G_1/N_1 \cong \bigoplus_{n \geq 1} \mathbb{Z} \cong \bigoplus_{n \geq 2} \mathbb{Z} = G_2/N_2.$$

Es gilt aber  $N_1 \not\cong N_2$ , denn  $N_1 \cong \mathbb{Z}$  ist zyklisch,  $\mathbb{Z} \oplus \mathbb{Z}$  aber nicht.

3. Es seien  $G_1 = \mathbb{Z}/4\mathbb{Z}$  und  $G_2 = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ , sowie  $N_1 = 2\mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{2}\}$  und  $N_2 = \mathbb{Z}/2\mathbb{Z} \oplus 0$ . Wegen der Kommutativität von  $G_1$  und  $G_2$  handelt es sich jeweils um eine normale Untergruppe. Da  $N_1$  und  $N_2$  beide zweielementig sind, gilt

$$N_1 \cong \mathbb{Z}/2\mathbb{Z} \cong N_2$$

(denn  $\mathbb{Z}/2\mathbb{Z}$  ist die bis auf Isomorphie eindeutige zweielementige Gruppe). Nach dem zweiten (oder dritten) Isomorphiesatz gilt

$$G_1/N_1 = (\mathbb{Z}/4\mathbb{Z})/(2\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z},$$

und für den anderen Quotienten gilt

$$\begin{aligned} G_2/N_2 &= (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z})/(\mathbb{Z}/2\mathbb{Z} \oplus 0) \\ &\cong ((\mathbb{Z}/2\mathbb{Z})/(\mathbb{Z}/2\mathbb{Z})) \oplus ((\mathbb{Z}/2\mathbb{Z})/0) \cong 0 \oplus \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}. \end{aligned}$$

Also gilt auch  $G_1/N_1 \cong G_2/N_2$ . Es gilt aber  $G_1 \not\cong G_2$ , da  $G_1$  ein Element der Ordnung 4 enthält,  $G_2$  jedoch nicht.

**Übung 4. Gruppen mit trivialer Automorphismengruppe**

Es sei  $G$  eine Gruppe mit  $\text{Aut}(G) = 1$ .

1. Zeigen Sie, dass  $G$  abelsch ist.
2. Zeigen Sie, dass  $g = -g$  für alle  $g \in G$ .
3. Folgern Sie, dass es eine eindeutige  $\mathbb{F}_2$ -Vektorraumstruktur auf  $G$  gibt.
4. Folgern Sie, dass  $G = 0$  oder  $G \cong \mathbb{Z}/2\mathbb{Z}$ .

**Lösung 4.**

1. Für  $g \in G$  sei  $c_g: G \rightarrow G$  die Konjugation mit  $g$ . Dies ist ein Automorphismus von  $G$ , weshalb  $c_g = \text{id}_G$ . Somit ist  $g \in Z(G)$ .
2. Wegen der Kommutativität von  $G$  ist die Abbildung  $n: G \rightarrow G, g \mapsto -g$  ein Automorphismus von  $G$ . Somit ist  $n = \text{id}_G$ , also  $-g = g$  für alle  $g \in G$ .
3. Nach dem vorherigen Aufgabenteil ist  $2g = 0$  für alle  $g \in G$ . Deshalb gibt es eine eindeutige  $\mathbb{F}_2$ -Vektorraumstruktur auf  $G$  via

$$\bar{n} \cdot g = n \cdot g \quad \text{für alle } n \in \mathbb{Z}, g \in G,$$

wie sich durch direktes Nachrechnen ergibt.

4. Es sei  $(b_i)_{i \in I}$  eine Basis von  $G$  als  $\mathbb{F}_2$ -Vektorraum. Ist  $G \neq 0$  und  $G \not\cong \mathbb{Z}/2$ , so ist  $\dim_{\mathbb{F}_2} G \geq 2$ . Es gibt daher  $i_1, i_2 \in I$  with  $i_1 \neq i_2$ . Die Permutation

$$\sigma: \{b_i\}_{i \in I} \rightarrow \{b_i\}_{i \in I}, \quad b_j \mapsto \begin{cases} b_{i_2} & \text{falls } j = i_1, \\ b_{i_1} & \text{falls } j = i_2, \\ b_j & \text{sonst,} \end{cases}$$

induziert einen nicht-trivialen  $\mathbb{F}_2$ -Vektorraumautomorphismus  $\alpha: G \rightarrow G$  mit

$$\alpha \left( \sum_{i \in I} \lambda_i b_i \right) = \sum_{i \in I} \lambda_i b_{\sigma(i)}.$$

Dann ist  $\alpha$  aber insbesondere ein nicht-trivialer Gruppenautomorphismus, im Widerspruch zu  $\text{Aut}(G) = 1$ .

## 2 Ringtheorie

**Übung 5.** *Initialobjekte in der Kategorie der Ringe*

1. Zeigen Sie, dass es für jeden Ring  $R$  einen eindeutigen Ringhomomorphismus  $\mathbb{Z} \rightarrow R$  gibt. (Dies bedeutet, dass der Ring  $\mathbb{Z}$  ein Initialobjekt in der Kategorie der Ringe ist.)
2. Es sei  $Z$  ein Ring, so dass es für jeden Ring  $R$  einen eindeutigen Ringhomomorphismus  $Z \rightarrow R$  gibt. Zeigen Sie, dass  $Z \cong \mathbb{Z}$ .

**Lösung 5.**

1. Ist  $\phi: \mathbb{Z} \rightarrow R$  ein Ringhomomorphismus, so ist  $\phi(1_{\mathbb{Z}}) = 1_R$ . Für alle  $n \in \mathbb{Z}$  ist damit

$$\phi(n) = \phi(n \cdot 1_{\mathbb{Z}}) = n \cdot \phi(1_{\mathbb{Z}}) = n \cdot 1_R.$$

Also ist  $\phi$  eindeutig. Durch direktes Nachrechnen ergibt sich auch, dass  $\psi: \mathbb{Z} \rightarrow R$  mit

$$\psi(n) := n \cdot 1_R \quad \text{für alle } n \in \mathbb{Z}$$

ein Ringhomomorphismus ist.

2. Es gibt einen eindeutigen Ringhomomorphismus  $\phi: \mathbb{Z} \rightarrow Z$  sowie einen eindeutigen Ringhomomorphismus  $\psi: Z \rightarrow \mathbb{Z}$ . Es ist auch  $\psi \circ \phi: \mathbb{Z} \rightarrow \mathbb{Z}$  ein Ringhomomorphismus. Die Identität  $\text{id}_{\mathbb{Z}}: \mathbb{Z} \rightarrow \mathbb{Z}$  ebenfalls ein Ringhomomorphismus ist. Da es genau einen Ringhomomorphismus  $\mathbb{Z} \rightarrow \mathbb{Z}$  gibt, muss sowohl  $\psi \circ \phi$  als auch  $\text{id}_{\mathbb{Z}}$  dieser eindeutige Ringhomomorphismus  $\mathbb{Z} \rightarrow \mathbb{Z}$  sein. Folglich ist  $\psi \circ \phi = \text{id}_{\mathbb{Z}}$ . Analog ergibt sich, dass  $\phi \circ \psi = \text{id}_Z$ .

**Übung 6.**

Es sei  $R$  ein Ring. Konstruieren Sie eine Bijektion zwischen der Menge der Ringhomomorphismen  $\mathbb{Z}[T] \rightarrow R$  und  $R$ .

**Lösung 6.**

Aus der Vorlesung ist bekannt, dass die Abbildung

$$\begin{aligned} \{\text{Ringhomomorphismen } \mathbb{Z}[T] \rightarrow R\} &\rightarrow \{\text{Ringhomomorphismen } \mathbb{Z} \rightarrow R\} \times R, \\ \phi &\mapsto (\phi|_{\mathbb{Z}}, \phi(T)) \end{aligned}$$

eine Bijektion ist. Da es genau einen Ringhomomorphismus  $\mathbb{Z} \rightarrow R$  gibt, ergibt sich ferner, dass die Abbildung

$$\{\text{Ringhomomorphismen } \mathbb{Z} \rightarrow R\} \times R \rightarrow R, \quad (\psi, r) \mapsto r$$

eine Bijektion ist. Damit ergibt sich insgesamt eine Bijektion

$$\{\text{Ringhomomorphismen } \mathbb{Z}[T] \rightarrow R\} \rightarrow R, \quad \phi \mapsto \phi(T).$$

### Übung 7.

Es sei  $R$  ein kommutativer Ring.

1. Zeigen Sie, dass ein Ideal  $\mathfrak{p} \subseteq R$  genau dann prim ist, wenn  $R/\mathfrak{p}$  ein Integritätsbereich ist.
2. Zeigen Sie, dass ein Ideal  $\mathfrak{m} \subseteq R$  genau dann maximal ist, wenn  $R/\mathfrak{m}$  ein Körper ist.

### Lösung 7.

Dies ist eine Standardaussage, deren Beweis sich in jedem Algebra-Buch findet.

### Übung 8.

Es sei  $R$  ein kommutativer Ring und  $I \subseteq R$  ein Ideal.

1. Definieren Sie das Radikal  $\sqrt{I}$  und zeigen Sie, dass  $\sqrt{I}$  ein Ideal mit  $I \subseteq \sqrt{I}$  ist.
2. Zeigen Sie, dass  $\sqrt{\sqrt{I}} = \sqrt{I}$ .
3. Zeigen Sie, dass  $\sqrt{I}$  genau dann ein echtes Ideal ist, wenn  $I$  ein echtes Ideal ist.

Ein Ideal  $I$  ist ein *Radikalideal*, wenn  $I = \sqrt{I}$  für ein Ideal  $J \subseteq I$ .

4. Zeigen Sie, dass  $I$  genau dann ein Radikalideal ist, wenn  $\sqrt{I} = I$ .

Ein Ring  $S$  heißt *reduziert*, falls 0 das einzige nilpotente Element von  $S$  ist.

5. Zeigen Sie, dass  $R/I$  genau dann reduziert ist, wenn  $I$  ein Radikalideal ist.
6. Zeigen Sie, dass jedes Primideal ein Radikalideal ist.

### Lösung 8.

1. Das Radikal  $\sqrt{I}$  ist als

$$\sqrt{I} = \{r \in R \mid \text{es gibt } n \in \mathbb{N} \text{ mit } r^n \in I\}$$

definiert. Für alle  $x \in I$  gilt  $x^1 = x \in I$ , weshalb  $I \subseteq \sqrt{I}$ .

Insbesondere ist somit  $0 \in \sqrt{I}$ , da  $0 \in I$ . Für  $x, y \in \sqrt{I}$  gibt es  $n, m \in \mathbb{N}$  mit  $x^n, y^m \in I$ . Für alle  $k = 0, \dots, n+m$  gilt deshalb  $x^k \in I$  oder  $y^{n+m-k} \in I$ , und somit auch

$$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k} \in I.$$

Deshalb ist auch  $x+y \in \sqrt{I}$ . Für  $r \in R$  und  $x \in I$  gibt es  $n \in \mathbb{N}$  mit  $x^n \in I$ , weshalb auch

$$(rx)^n = r^n x^n \in I.$$

Somit ist auch  $rx \in \sqrt{I}$ .

2. Wir wissen bereits, dass  $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$ . Für  $x \in \sqrt{\sqrt{I}}$  gibt es  $n \in \mathbb{N}$  mit  $x^n \in \sqrt{I}$ , und somit auch noch  $m \in \mathbb{N}$  mit  $(x^n)^m \in I$ . Damit ist  $x^{nm} \in I$ , weshalb auch  $\sqrt{\sqrt{I}} \subseteq \sqrt{I}$ .
3.  $I$  ist genau dann ein echtes Ideal, wenn  $1 \notin I$ . Da  $1^n = 1$  für alle  $n \in \mathbb{N}$  ist genau dann  $1 \notin I$ , wenn  $1 \notin \sqrt{I}$ . Dies ist wiederum äquivalent dazu, dass  $\sqrt{I}$  ein echtes Ideal ist.
4. Gilt  $I = \sqrt{I}$  so erfüllt  $I$  die definierende Eigenschaft eines Radikalideals (mit  $J = I$ ). Ist andererseits  $I = \sqrt{J}$  für ein Ideal  $J \subseteq R$ , so gilt

$$\sqrt{I} = \sqrt{\sqrt{J}} = \sqrt{J} = I.$$

5. Der Quotient  $R/I$  ist genau reduziert, wenn

$$\text{es gibt } n \in \mathbb{N} \text{ mit } \bar{x}^n = 0 \implies \bar{x} = 0 \quad \text{für alle } x \in R. \quad (1)$$

Dabei gilt  $\bar{x}^n = \overline{x^n}$  für alle  $x \in R$  und  $n \in \mathbb{N}$ , und für alle  $y \in R$  gilt genau dann  $\bar{y} = 0$ , wenn  $y \in I$ . Daher ist (1) äquivalent dazu, dass

$$\text{es gibt } n \in \mathbb{N} \text{ mit } x^n \in I \implies x \in I \quad \text{für alle } x \in R. \quad (2)$$

Durch Einsetzen der Definition von  $\sqrt{I}$  ergibt sich aus (2) die äquivalente Bedingung

$$x \in \sqrt{I} \implies x \in I \quad \text{für alle } x \in R.$$

Dies bedeutet gerade, dass  $\sqrt{I} \subseteq I$ . Da  $I \subseteq \sqrt{I}$  ist dies äquivalent dazu, dass  $I = \sqrt{I}$ , dass also  $I$  ein Radikalideal ist.

6. Der Quotient  $R/\mathfrak{p}$  ist ein Integritätsbereich, da  $\mathfrak{p}$  ein Primideal ist. Nach dem vorherigen Aufgabenteil genügt es zu zeigen, dass jeder Integritätsbereich  $S$  reduziert ist. Dies folgt direkt daraus, dass für jedes  $x \in S$  mit  $x^n = 0$  aus der Nullteilerfreiheit von  $S$  folgt, dass  $x = 0$ .

### Übung 9.

Es sei  $R$  ein kommutativer Ring und  $\mathfrak{p} \subseteq R$  ein Ideal. Zeigen Sie, dass  $\mathfrak{p}$  genau dann ein Primideal ist, wenn es einen Körper  $K$  und einen Ringhomomorphismus  $\phi: R \rightarrow K$  mit  $\ker \phi = \mathfrak{p}$  gibt.

### Lösung 9.

Ist  $\mathfrak{p}$  ein Primideal, so ist der Quotient  $R/\mathfrak{p}$  ein Integritätsbereich. Da die kanonische Inklusion  $R/\mathfrak{p} \rightarrow Q(R/\mathfrak{p})$  ein injektiver Ringhomomorphismus ist, folgt für die Komposition

$$\phi: R \xrightarrow{\pi} R/\mathfrak{p} \rightarrow Q(R/\mathfrak{p}),$$

dass  $\ker \phi = \ker \pi = \mathfrak{p}$ . (Hier bezeichnet  $\pi: R \rightarrow R/\mathfrak{p}$  die kanonische Projektion.) Da  $Q(R/\mathfrak{p})$  ein Körper ist, zeigt dies eine Implikation.

Gibt es andererseits einen Körper  $K$  und einen Ringhomomorphismus  $\phi: R \rightarrow K$  mit  $\mathfrak{p} = \ker \phi$ , so ist  $R/\mathfrak{p} \cong \text{im } \phi \subseteq K$ . Der Körper  $K$  ist insbesondere ein Integritätsbereich,



weshalb auch der Unterring  $\phi$  ein Integritätsbereich ist. Der Quotient  $R/\mathfrak{p}$  ist also ein Integritätsbereich und  $\mathfrak{p}$  somit eine Primideal.

### Übung 10.

Es sei  $K$  ein Körper.

1. Zeigen Sie, dass es für jedes Polynom  $f \in K[X]$  einen eindeutigen  $K$ -linearen Ringhomomorphismus  $\phi_f: K[X] \rightarrow K[X]$  gibt, so dass  $\phi_f(X) = f$ .  
(Hinweis: Zeigen Sie zunächst, dass  $\phi_f|_K = \text{id}_K$  gilt.)
2. Zeigen Sie, dass  $\phi_f$  genau dann ein Ringisomorphismus ist, wenn  $\deg f = 1$ .

### Übung 11. Funktorialität der Einheitengruppe

Ist  $R$  ein kommutativer Ring, so ist

$$R^\times := \{x \in R \mid x \text{ ist eine Einheit}\}$$

die Einheitengruppe von  $R$ . Zeigen Sie:

1. Ist  $R$  ein kommutativer Ring, so bildet  $R^\times$  mit der Multiplikation aus  $R$  eine abelsche Gruppe.
2. Sind  $R$  und  $S$  zwei kommutativer Ringe und ist  $\phi: R \rightarrow S$  ein Ringhomomorphismus, so induziert  $\phi$  per Einschränkung einen Gruppenhomomorphismus

$$\phi^\times: R^\times \rightarrow S^\times, \quad x \mapsto \phi(x).$$

3. Für jeden Ring kommutativen  $R$  gilt  $\text{id}_R^\times = \text{id}_{R^\times}$ , und für alle kommutativen Ringe  $R_1, R_2$  und  $R_3$  und Ringhomomorphismen  $\phi: R_1 \rightarrow R_2$  und  $\psi: R_2 \rightarrow R_3$  gilt  $(\psi\phi)^\times = \psi^\times \phi^\times$ .
4. Ist  $R$  ein kommutativer Ring und  $\phi: R \rightarrow S$  ein Isomorphismus von Ringen, so ist  $\phi^\times: R^\times \rightarrow S^\times$  ein Isomorphismus von Gruppen.

(Die Aussagen gelten auch für nichtkommutative Ringe, wobei  $R^\times$  dann im Allgemeinen nicht abelsch ist. Dabei ist ein Element  $r \in R$  eines nichtkommutativen Rings  $R$  eine Einheit, wenn es  $s \in R$  mit  $rs = 1 = sr$  gibt. Es genügt auch, dass es  $s, t \in R$  mit  $rs = 1 = tr$  gibt; dann gilt bereits  $s = t$ .)

### Lösung 11.

1. Die Multiplikation in  $R^\times$  ist assoziativ, da sie es in  $R$  ist. Dass  $R^\times$  abelsch ist ergibt sich aus der Kommutativität von  $R$ . Es gilt  $1 \in R^\times$ , und da 1 in ganz  $R$  neutral bezüglich der Multiplikation ist, gilt dies auch in  $R^\times$ . Für jedes  $x \in R^\times$  gibt es ein  $y \in R$  mit  $xy = 1$ . Dann gilt auch  $y \in R^\times$  und  $y$  ist auch in  $R^\times$  invers zu  $x$ .
2. Für  $x \in R^\times$  gilt

$$1 = \phi(1) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1}).$$

Deshalb ist  $\phi(x)$  eine Einheit in  $S$  (mit  $\phi(x)^{-1} = \phi(x^{-1})$ ), und somit  $\phi(x) \in S^\times$ . Das zeigt, dass die Einschränkung  $\phi^\times$  wohldefiniert ist. Da  $\phi$  multiplikativ ist, gilt dies auch für  $\phi^\times$ , weshalb  $\phi^\times$  ein Gruppenhomomorphismus ist.

3. Da  $\text{id}_R^\times(x) = \text{id}_R(x) = x = \text{id}_{R^\times}(x)$  für alle  $x \in X$  gilt, ist  $\text{id}_R^\times = \text{id}_{R^\times}$ . Für alle  $x \in R_1$  gilt

$$(\psi^\times \phi^\times)(x) = \psi^\times(\phi^\times(x)) = \psi(\phi(x)) = (\psi\phi)(x) = (\psi\phi)^\times(x).$$

Deshalb ist  $(\psi^\times \phi^\times) = (\psi\phi)^\times$ .

4. Es sei  $\psi := \phi^{-1}: S \rightarrow R$ . Es gilt

$$\phi^\times \psi^\times = (\phi\psi)^\times = (\phi\phi^{-1})^\times = \text{id}_S^\times = \text{id}_{S^\times}$$

und analog auch  $\psi^\times \phi^\times = \text{id}_{R^\times}$ . Also ist der Gruppenhomomorphismus  $\phi^\times$  bijektiv mit  $(\phi^\times)^{-1} = (\phi^{-1})^\times$ , und somit ein Gruppenisomorphismus.

### Übung 12. Urbilder von Idealen

Es seien  $R$  und  $S$  zwei kommutative Ringe und  $\phi: R \rightarrow S$  ein Ringhomomorphismus.

1. Zeigen Sie, dass für jedes Ideal  $\mathfrak{a} \subseteq S$  das Urbild  $\phi^{-1}(\mathfrak{a})$  ein Ideal in  $R$  ist.
2. Entscheiden Sie, ob  $\phi^{-1}(\mathfrak{p})$  ein Primideal ist, wenn  $\mathfrak{p} \subseteq S$  ein Primideal ist.
3. Entscheiden Sie, ob  $\phi^{-1}(\mathfrak{m})$  ein maximales Ideal ist, wenn  $\mathfrak{m} \subseteq S$  ein maximales Ideal ist.

### Lösung 12.

1. Es sei  $\pi: S \rightarrow S/\mathfrak{a}$ ,  $s \mapsto \bar{s}$  die kanonische Projektion. Dann ist  $\pi\phi$  ein Ringhomomorphismus und somit  $\ker(\pi\phi) = \phi^{-1}(\ker \pi) = \phi^{-1}(\mathfrak{a})$  ein Ideal in  $R$ .
2. Die Aussage gilt: Es sei  $\pi: S \rightarrow S/\mathfrak{p}$ ,  $s \mapsto \bar{s}$  die kanonische Projektion und  $\mathfrak{q} := \phi^{-1}(\mathfrak{p})$ . Der Quotient  $S/\mathfrak{p}$  ist ein Integritätsbereich, da  $\mathfrak{p}$  ein Primideal ist. Nach dem vorherigen Aufgabenteil ist  $\mathfrak{q}$  ein Ideal in  $R$ , und da  $\ker(\pi\phi) = \phi^{-1}(\ker \pi) = \phi^{-1}(\mathfrak{p}) = \mathfrak{q}$  induziert  $\pi\phi$  einen injektiven Ringhomomorphismus

$$\psi: R/\mathfrak{q} \rightarrow S/\mathfrak{p} \quad \bar{r} \mapsto \overline{\phi(r)}.$$

Der Ring  $\text{im}(\pi\phi) \subseteq S/\mathfrak{p}$  ist als Unterring eines Integritätsbereichs ebenfalls ein Integritätsbereich. Somit ist  $R/\mathfrak{q} \cong \text{im}(\pi\phi)$  ein Integritätsbereich, also  $\mathfrak{q}$  ein Primideal.

3. Die Aussage gilt nicht: Es sei etwa  $\phi: \mathbb{Z} \rightarrow \mathbb{Q}$  die kanonische Inklusion. Dann ist  $\mathfrak{m} := 0$  ein maximales Ideal in  $\mathbb{Q}$ , aber  $\phi^{-1}(0) = 0$  ist kein maximales Ideal in  $\mathbb{Z}$ , da  $\mathbb{Z}/\mathfrak{m} \cong \mathbb{Z}$  kein Körper ist.

### Übung 13.

Es sei  $R$  ein kommutativer Ring. Es seien  $\mathfrak{a}, \mathfrak{b} \subseteq R$  zwei Ideale mit  $\mathfrak{a} = (x_i \mid i \in I)$  und  $\mathfrak{b} = (y_j \mid j \in J)$ . Zeigen Sie, dass

$$\mathfrak{a}\mathfrak{b} = (x_i y_j \mid i \in I, j \in J).$$

**Lösung 13.**

Für alle  $i \in I$  und  $j \in J$  folgt aus  $x_i \in \mathfrak{a}$  und  $y_j \in \mathfrak{b}$ , dass  $x_i y_j \in \mathfrak{ab}$ . Daraus folgt, dass  $(x_i y_j \mid i \in I, j \in J) \subseteq \mathfrak{ab}$ . Sind andererseits  $a \in \mathfrak{a}$  und  $b \in \mathfrak{b}$ , so ist  $a = \sum_{i \in I} r_i x_i$  und  $b = \sum_{j \in J} s_j y_j$  mit  $r_i, s_j \in R$ , wobei  $r_i = 0$  für fast alle  $i \in I$  und  $s_j = 0$  für fast alle  $j \in J$ . Deshalb ist

$$ab = \sum_{\substack{i \in I \\ j \in J}} r_i s_j x_i y_j \in (x_i y_j \mid i \in I, j \in J).$$

Da jedes Element aus  $\mathfrak{ab}$  von der Form  $\sum_{k=1}^n a_k b_k$  mit  $a_k \in \mathfrak{a}$  und  $b_k \in \mathfrak{b}$  ist, folgt daraus, dass  $\mathfrak{ab} \subseteq (x_i y_j \mid i \in I, j \in J)$ .

**Übung 14.** Zur Definition von Unterringen

Geben Sie ein Beispiel für einen kommutativen Ring  $R$  und eine Teilmenge  $S \subseteq R$  mit den folgenden Eigenschaften:

- $S$  ist abgeschlossen unter der Addition und Multiplikation von  $R$ , d.h. für alle  $s_1, s_2 \in S$  ist auch  $s_1 + s_2 \in S$  und  $s_1 s_2 \in S$ .
- Zusammen mit der Einschränkung der Addition und Multiplikation aus  $R$  ist  $S$  ebenfalls ein (notwendigerweise kommutativer) Ring.
- $S$  ist kein Unterring von  $R$ .

**Lösung 14.**

Es sei  $R = \mathbb{Z} \times \mathbb{Z}$  und  $S = \mathbb{Z} \times 0 = \{(n, 0) \mid n \in \mathbb{Z}\}$ . Offenbar ist  $S$  unter der Addition und Multiplikation abgeschlossen. Zusammen mit der Einschränkung dieser Operationen bildet  $S$  einen kommutativen Ring, für den  $S \cong \mathbb{Z}$  gilt. Da  $1_R = (1, 1) \notin S$  ist  $S$  allerdings kein Unterring von  $R$ .

**Übung 15.**

Es sei  $R$  ein kommutativer Ring.

1. Definieren Sie, wann zwei Elemente von  $R$  assoziiert sind.
2. Zeigen Sie, dass Assoziiertheit eine Äquivalenzrelation ist.
3. Es sei nun  $R$  ein Integritätsbereich. Zeigen Sie, dass zwei Elemente  $a, b \in R$  genau dann assoziiert sind, wenn  $(a) = (b)$ .

**Lösung 15.**

1. Ein Element  $y \in R$  ist assoziiert zu einem Element  $x \in R$ , wenn es eine Einheit  $\varepsilon \in R^\times$  mit  $y = \varepsilon x$  gibt.

Für  $x, y \in R$  schreiben wir im Folgenden  $x \sim y$ , wenn  $y$  assoziiert zu  $x$  ist.

2. Für jedes  $x \in R$  ist  $x \sim x$  da  $x = 1 \cdot x$  mit  $1 \in R^\times$ . Für  $x, y \in R$  mit  $x \sim y$  gibt es  $\varepsilon \in R^\times$  mit  $y = \varepsilon x$ ; dann ist  $\varepsilon^{-1} \in R^\times$  mit  $x = \varepsilon^{-1}y$  und deshalb  $y \sim x$ . Für  $x, y, z \in R$  mit  $x \sim y$  und  $y \sim z$  gibt es  $\varepsilon_1, \varepsilon_2 \in R^\times$  mit  $y = \varepsilon_1 x$  und  $z = \varepsilon_2 y$ ; dann ist  $\varepsilon_2 \varepsilon_1 \in R^\times$  mit  $z = \varepsilon_2 y = \varepsilon_2 \varepsilon_1 x$  und somit  $x \sim z$ .

3. Für  $x, y \in R$  mit  $x \sim y$  gibt es  $\varepsilon \in R^\times$  mit  $x = \varepsilon y$ . Dann ist  $R\varepsilon = R$  und deshalb

$$(x) = \{rx \mid r \in R\} = \{r\varepsilon y \mid r \in R\} = \{r'y \mid r' \in R\varepsilon\} = \{r'y \mid r' \in R\} = (y).$$

Ist andererseits  $(x) = (y)$  so ist  $x \in (y)$  und  $y \in (x)$ , also gibt es  $\varepsilon_1, \varepsilon_2 \in R$  mit  $y = \varepsilon_1 x$  und  $x = \varepsilon_2 y$ . Dann ist  $y = \varepsilon_1 x = \varepsilon_1 \varepsilon_2 y$ , und da  $R$  ein Integritätsbereich ist, somit  $\varepsilon_1 \varepsilon_2 = 1$ . Also ist  $\varepsilon_1$  eine Einheit mit  $\varepsilon_1^{-1} = \varepsilon_2$ . Da  $y = \varepsilon_1 x$  ist  $x \sim y$ .

### Übung 16.

Es sei  $R$  ein kommutativer Ring und  $S \subseteq R$  eine multiplikative Teilmenge.

1. Zeigen Sie, dass  $R_S$  noethersch ist, wenn  $R$  noethersch ist.
2. Zeigen oder widerlegen Sie, dass  $R_S$  ein Hauptidealring ist, wenn  $R$  ein Hauptidealring ist.

### Übung 17.

Es sei  $R$  ein Ring und  $I \subseteq R$  ein Ideal.

1. Zeigen Sie, dass  $R/I$  noethersch ist, wenn  $R$  noethersch ist.
2. Zeigen Sie widerlegen, dass  $R/I$  ein Hauptidealring ist, wenn  $R$  ein Hauptidealring ist.

### Übung 18.

Für jedes  $d \in \mathbb{N}$  sei

$$\mathbb{Z}[\sqrt{-d}] := \mathbb{Z}[i\sqrt{d}] = \{a + i\sqrt{d}b \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

Es darf im Folgenden ohne Beweis genutzt werden, dass  $\mathbb{Z}[\sqrt{-d}]$  ein Unterring von  $\mathbb{C}$  ist.

1. Zeigen Sie, dass  $\mathbb{Z}[\sqrt{-1}]$  ein euklidischer Ring ist.
2. Zeigen Sie, dass  $\mathbb{Z}[\sqrt{-2}]$  ein euklidischer Ring ist.
3. Zeigen Sie, dass  $\mathbb{Z}[\sqrt{-5}]$  kein euklidischer Ring ist.

### Übung 19.

Es sei  $R$  ein euklidischer Ring. Zeigen Sie, dass  $R$  ein Hauptidealring ist.

**Lösung 19.**

Als euklidischer Ring ist  $R$  insbesondere ein Integritätsbereich. Es sei  $g: R \rightarrow \mathbb{N}$  die Gradabbildung und  $I \subseteq R$  ein Ideal. Ist  $I = 0$  so ist  $I = (0)$ , wir betrachten daher den Fall  $I \neq 0$ . Dann gibt es ein bezüglich  $g$  minimales  $a \in I$ , d.h.  $a \in I$  mit  $a \neq 0$  und  $g(a) \leq g(x)$  für alle  $x \in I$  mit  $x \neq 0$ . Es gilt  $(a) \subseteq I$  und es handelt sich bereits um Gleichheit: Ist  $x \in I$  so gibt es  $b, r \in R$  mit  $x = ab + r$ , und entweder  $r = 0$  oder  $g(r) < g(a)$ . Da  $r = x - ab \in I$  kann  $g(r) < g(a)$  wegen der Minimalität von  $a$  nicht eintreten. Also ist  $r = 0$  und somit  $x = ab \in (a)$ .

**Übung 20.**

Es sei  $K$  ein kommutativer Ring, so dass  $K[X]$  ein Hauptidealring ist. Zeigen Sie, dass  $K$  bereits ein Körper ist.

**Lösung 20.**

Wir geben zwei mögliche Beweise:

1. Es sei  $a \in K$  mit  $a \neq 0$ . Das Ideal  $(a, X)$  ist nach Annahme ein Hauptideal. Also gibt es ein Polynom  $f \in K[X]$  mit

$$(a, X) = (f). \quad (3)$$

Wegen Gleichung (3) gilt  $f \mid a$ , d.h. es gibt  $g \in K[X]$  mit  $fg = a$ . Entscheidend ist nun die folgende Beobachtung:

**Behauptung 1.** Die übliche Gradabbildung  $\deg: K[X] \rightarrow \mathbb{N}$  ist additiv.

*Beweis.* As Hauptidealring ist  $K[X]$  insbesondere ein Integritätsbereich. Also ist auch der Unterring  $K \subseteq K[X]$  ein Integritätsbereich, woraus die Aussage folgt.  $\square$

Aus Behauptung 1 erhalten wir, dass

$$0 = \deg(a) = \deg(fg) = \deg(f) + \deg(g).$$

Es muss  $\deg(f) = \deg(g) = 0$  gelten und somit bereits  $f, g \in K$ .

Da  $f \in (a, X)$  gibt es  $p, q \in K[X]$  mit  $f = ap + Xq$ . Da  $f \in K$  und  $\deg(Xq) \geq 1$  ergibt sich durch Vergleich des 0-ten Koeffizienten, dass  $f = f_0 = a_0p_0 = ap_0$ . Deshalb gilt bereits  $f = ap_0 \in (a)$ . Wir haben also

$$(a, X) = (f) \subseteq (a) \subseteq (a, X)$$

und somit  $(a, X) = (a)$ .

Es gibt deshalb  $h \in K[X]$  mit  $X = ah$ . Durch Gradvergleich erhalten wir, dass

$$1 = \deg(X) = \deg(ah) = \deg(a) + \deg(h) = 0 + \deg(h) = \deg(h)$$

und deshalb  $h(X) = b_1X + b_0$  für  $b_1, b_0 \in K$ . Durch Koeffizientenvergleich erhalten wir aus der Gleichung

$$X = ah(X) = a(b_1X + b_0) = ab_1X + ab_0,$$

dass  $ab_1 = 1$ . Das zeigt, dass  $a \in A$  eine Einheit ist.

2. Der obige Beweis lässt sich leicht ändern. Wir zeigen, dass das Ideal  $(X)$  maximal ist. Ansonsten gebe es  $a \in K[X]$ , so dass  $(X) \subsetneq (a, X) \subsetneq K[X]$ . Da  $(a, X) = (a_0, X)$  können o.B.d.A. davon ausgehen, dass  $a \in K$ . Wie zuvor ergibt sich, dass  $(a, X) = (X)$ , was  $(X) \subsetneq (a, X)$  widerspricht. Also ist  $(X)$  maximal, und  $K \cong K[X]/(X)$  somit ein Körper.

Der erste Beweis hat den Vorteil, dass er für einen beliebigen kommutativen Ring  $R$  zeigt, dass  $(a, X)$  für  $a \in R$  genau dann ein Hauptidealring ist, wenn  $a \in R^\times$ . Somit ist beispielsweise  $(2, X) \subseteq \mathbb{Z}[X]$  kein Hauptideal.

#### Übung 21.

Es sei  $K$  ein Körper. Zeigen Sie, dass es in  $K[X]$  unendlich viele irreduzible, normierte Polynome gibt.

#### Übung 22.

Es seien  $R$  und  $R'$  zwei kommutative Ringe,  $S \subseteq R$  eine multiplikative Teilmenge und  $f: R \rightarrow R'$  ein Ringhomomorphismus.

1. Zeigen Sie, dass  $S' := f(S)$  eine multiplikative Teilmenge von  $R'$  ist.
2. Zeigen Sie, dass  $f$  einen Ringhomomorphismus  $f_S: R_S \rightarrow R'_{S'}$  induziert.

#### Lösung 22.

1. Da  $1 \in S$  ist  $1 = f(1) \in f(S) = S'$ . Für  $s'_1, s'_2 \in S'$  gibt es  $s_1, s_2 \in S$  mit  $s'_1 = f(s_1)$  und  $s'_2 = f(s_2)$ , und damit ist auch  $s'_1 s'_2 = f(s_1) f(s_2) = f(s_1 s_2) \in f(S) = S'$ .
2. Es seien  $i: R \rightarrow R_S, r \mapsto r/1$  und  $i': R' \rightarrow R'_{S'}, r' \mapsto r'/1$  die kanonischen Ringhomomorphismen. Die Komposition  $i' \circ f: R \rightarrow R'_{S'}$  bildet  $s \in S$  auf die Einheit  $f(s)/1 \in R'_{S'}$  ab. Nach der universellen Eigenschaft der Lokalisierung induziert  $i' \circ f$  einen eindeutigen Ringhomomorphismus  $f_S: R_S \rightarrow R'_{S'}$  mit  $f_S i = i' f$ , d.h. so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ \downarrow i & & \downarrow i' \\ R_S & \xrightarrow{f_S} & R'_{S'} \end{array}$$

#### Übung 23.

Es sei  $R$  ein kommutativer Ring.

1. Zeigen Sie, dass für jedes Ideal  $\mathfrak{a} \subseteq R$  die Teilmenge

$$\mathfrak{a}[X] := \left\{ \sum_i f_i X^i \in R[X] \mid f_i \in \mathfrak{a} \text{ für alle } i \right\}$$

ein Ideal in  $R[X]$  ist.

2. Zeigen Sie, dass  $\mathfrak{p}[X]$  ein Primideal in  $R[X]$ , wenn  $\mathfrak{p} \subseteq R$  ein Primideal ist.
3. Zeigen oder widerlegen Sie, dass  $\mathfrak{m}[X]$  notwendigerweise ein maximales Ideal in  $R[X]$  ist, wenn  $\mathfrak{m} \subseteq R$  ein maximales Ideal ist.

**Lösung 23.**

1. Die kanonische Projektion  $\pi: R \rightarrow R/\mathfrak{a}$ ,  $x \mapsto \bar{x}$  induziert nach der universellen Eigenschaft des Polynomrings  $R[X]$  einen Ringhomomorphismus  $\varphi: R[X] \rightarrow (R/\mathfrak{a})[X]$  mit  $\varphi|_R = \pi$  und  $\varphi(X) = \pi(X)$ , und dieser ist gegeben durch

$$\varphi\left(\sum_i f_i X^i\right) = \sum_i \pi(f_i) X^i = \sum_i \bar{f}_i X^i.$$

Für  $f = \sum_i f_i X^i \in R[X]$  ist genau dann  $f \in \ker \varphi$ , wenn  $\bar{f}_i = 0$  für alle  $i$ , also genau dann, wenn  $f_i \in \ker \pi = \mathfrak{a}$  für alle  $i$ . Somit ist  $\ker \varphi = \mathfrak{a}[X]$  ein Ideal in  $R[X]$ .

2. Es seien  $\pi$  und  $\varphi$  wie zuvor. Wegen der Surjektivität von  $\pi$  ist auch  $\varphi$  surjektiv. Somit induziert  $\varphi$  einen Ringisomorphismus

$$\psi: R[X]/\mathfrak{p}[X] \rightarrow (R/\mathfrak{p})[X], \quad \overline{\sum_i f_i X^i} \mapsto \sum_i \bar{f}_i X^i.$$

Der Quotient  $R/\mathfrak{p}$  ist ein Integritätsbereich, da  $\mathfrak{p}$  ein Primideal in  $R$  ist. Somit ist auch  $(R/\mathfrak{p})[X]$  ein Integritätsbereich. Da der Quotient  $R[X]/\mathfrak{a}[X]$  ein Integritätsbereich ist, folgt, dass  $\mathfrak{p}[X]$  ein Primideal in  $R[X]$  ist.

3. Ist  $K$  ein Körper, so ist  $0 \subseteq K$  ein maximales Ideal, und es gilt  $\mathfrak{m}[X] = 0$ . Der Quotient  $K[X]/\mathfrak{m}[X] \cong (K/0)[X] \cong K[X]$  ist kein Körper, da  $0 \neq X \in K[X]$  keine Einheit ist. Also ist  $\mathfrak{m}[X]$  nicht maximal in  $K[X]$ .

Tatsächlich kann  $\mathfrak{m}[X]$  nicht maximal in  $R[X]$  sein, da  $R[X]/\mathfrak{m}[X] \cong (R/\mathfrak{m})[X]$ , aber es keinen Ring  $R'$  gibt, so dass  $R'[X]$  ein Körper ist (siehe Übung 24).

**Übung 24.**

Zeigen Sie, dass es keinen Ring  $R$  gibt, so dass  $R[X]$  ein Körper ist.

**Lösung 24.**

Gebe es einen solchen Ring  $R$ , so wäre  $R$  kommutativ, da  $R \subseteq R[X]$  ein Unterring ist. Es wäre auch  $R \neq 0$  da  $0[X] = 0$  kein Körper ist. Dann wäre aber  $0 \neq X \in R[X]$  keine Einheit und  $R[X]$  somit kein Körper.

**Übung 25.**

Zeigen Sie, dass  $\mathbb{Z}[i] \cong \mathbb{Z}[X]/(X^2 + 1)$ .

**Übung 26.**

Es sei  $R$  ein kommutativer Ring und  $f \in R$ . Zeigen Sie, dass  $R_f \cong R[X]/(fX - 1)$ .

**Lösung 26.**

Das Element  $\bar{f} \in R[X]/(fX - 1)$  ist eine Einheit mit  $\bar{f}^{-1} = \bar{X}$  da

$$\bar{f} \bar{X} = \overline{fX} = \bar{1} = 1.$$

Nach der universellen Eigenschaft der Lokalisierung  $R_f$  induziert der Ringhomomorphismus  $R \rightarrow R[X] \rightarrow R[X]/(fX - 1)$  einen Ringhomomorphismus  $\varphi: R_f \rightarrow R[X]/(fX - 1)$  mit

$$\varphi\left(\frac{r}{f^k}\right) = \frac{\bar{r}}{\bar{f}^k} = \bar{r} \bar{X}^k = \overline{rX^k}.$$

Andererseits induziert der kanonische Ringhomomorphismus  $i: R \rightarrow R_f, r \mapsto r/1$  nach der universellen Eigenschaft des Polynomrings  $R[X]$  einen eindeutigen Ringhomomorphismus  $\tilde{\psi}: R[X] \rightarrow R_f$  mit  $\tilde{\psi}|_R = i$  und  $\tilde{\psi}(X) = 1/f$ , und dieser ist gegeben durch

$$\tilde{\psi}\left(\sum_i r_i X^i\right) = \sum_i \frac{r_i}{f^i}.$$

Dann gilt insbesondere

$$\tilde{\psi}(fX - 1) = \tilde{\psi}(f)\tilde{\psi}(X) - \tilde{\psi}(1) = \frac{f}{1} \frac{1}{f} - \frac{1}{1} = 0.$$

Also faktorisiert  $\tilde{\psi}$  über einen eindeutigen Ringhomomorphismus  $\psi: R[X]/(fX - 1) \rightarrow R_f$  mit  $\psi(\bar{p}) = \tilde{\psi}(p)$  für alle  $p \in R[X]$ , d.h. es ist

$$\psi\left(\overline{\sum_i r_i X^i}\right) = \sum_i \frac{r_i}{f^i} \quad \text{für alle } \sum_i r_i X^i \in R[X].$$

Die beiden Ringhomomorphismen  $\varphi$  und  $\psi$  sind invers zueinander: Für alle  $r/f^k \in R_f$  gilt

$$\psi\left(\varphi\left(\frac{r}{f^k}\right)\right) = \psi\left(\overline{rX^k}\right) = \frac{r}{f^k},$$

und für alle  $\sum_i r_i X^i \in R[X]$  gilt

$$\varphi\left(\psi\left(\overline{\sum_i r_i X^i}\right)\right) = \varphi\left(\sum_i \frac{r_i}{f^i}\right) = \sum_i \varphi\left(\frac{r_i}{f^i}\right) = \overline{\sum_i r_i X^i}.$$

Also ist  $\varphi$  ein Isomorphismus mit  $\varphi^{-1} = \psi$ .



**Übung 27.**

Bestimmen Sie die Einheitengruppe  $\mathbb{Z}[i]^\times$ .

**Lösung 27.**

Ein Element  $z \in \mathbb{Z}[i]$  ist genau dann eine Einheit in  $\mathbb{Z}[i]$ , wenn  $z \neq 0$  und  $z^{-1} \in \mathbb{Z}[i]$  (hier bezeichnet  $z^{-1} = 1/z$  das Inverse von  $z$  in  $\mathbb{C}$ ). Für die Elemente  $1, -1, i, -i \in \mathbb{Z}[i]$  ist dies erfüllt. Ist  $z \in \mathbb{Z}[i]$  mit  $z \neq 0$  und  $z^{-1} \in \mathbb{Z}[i]$ , so ist

$$1 = |1|^2 = |zz^{-1}|^2 = |z|^2 |z^{-1}|^2. \quad (4)$$

Für alle  $w \in \mathbb{Z}[i]$  mit  $w = a + ib$  gilt  $a, b \in \mathbb{Z}$  und deshalb  $|w|^2 = a^2 + b^2 \in \mathbb{Z}$ . In (4) gilt deshalb, dass  $|z|^2, |z^{-1}|^2 \in \mathbb{Z}$ , und somit  $|z|^2 \in \mathbb{Z}^\times = \{1, -1\}$ . Also gilt  $|z|^2 = 1$ . Ist  $z = a + ib$  mit  $a, b \in \mathbb{Z}$  so ist also  $a^2 + b^2 = 1$  und somit entweder  $a = 0$  und  $b = \pm 1$ , oder  $a = \pm 1$  und  $b = 0$ . Es ist also  $z \in \{1, -1, i, -i\}$ . Insgesamt zeigt dies, dass  $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$ .

**Übung 28.**

Formulieren und beweisen Sie den Hilbertschen Basissatz.

### 3 Modultheorie

#### Übung 29.

Zeigen Sie, dass es auf jeder abelschen Gruppe genau eine  $\mathbb{Z}$ -Modulstruktur gibt.

#### Lösung 29.

Es sei  $A$  eine abelsche Gruppe. Aus der Vorlesung ist die Bijektion

$$\begin{aligned} \{\mathbb{Z}\text{-Modulstrukturen } \mathbb{Z} \times A \rightarrow A\} &\longleftrightarrow \{\text{Ringhomomorphismen } \mathbb{Z} \rightarrow \text{End}(A)\}, \\ \mu &\longmapsto (n \mapsto (a \mapsto \mu(n, a))), \\ ((n, a) \mapsto \phi(n)(a)) &\longleftarrow \phi. \end{aligned}$$

bekannt. Dabei ist

$$\text{End}(A) = \{f: A \rightarrow A \mid f \text{ ist additiv}\}$$

ein Ring unter punktweiser Addition und Komposition. Da es genau einen Ringhomomorphismus  $\mathbb{Z} \rightarrow \text{End}(A)$  gibt (siehe Übung 5) folgt die Aussage.

#### Übung 30.

Es sei  $R$  ein kommutativer Ring und  $M$  ein  $R$ -Modul. Es sei  $I \subseteq R$  ein Ideal.

1. Zeigen Sie, dass sich die  $R$ -Modulstruktur auf  $M$  genau dann zu einer  $R/I$ -Modulstruktur fortsetzen lässt, wenn  $IM = 0$  (d.h. wenn  $am = 0$  für alle  $a \in I$  und  $m \in M$ ).
2. Es sei  $S \subseteq R$  eine multiplikative Teilmenge. Zeigen Sie, dass sich die  $R$ -Modulstruktur auf  $M$  genau dann zu einer  $R_S$ -Modulstruktur fortsetzen lässt, wenn für jedes  $s \in S$  die Abbildung  $\lambda_s: M \rightarrow M, m \mapsto sm$  bijektiv ist.

#### Übung 31.

Es sei  $M$  ein endlich erzeugter  $R$ -Modul. Zeigen Sie, dass jedes Erzeugendensystem  $S \subseteq M$  ein endliches Erzeugendensystem enthält.

#### Lösung 31.

Es sei  $\{m_1, \dots, m_s\} \subseteq M$  ein endliches Erzeugendensystem. Da  $S$  ein Erzeugendensystem ist, lässt sich jedes  $m_i$  als  $m_i = r_{i,1}s_{i,1} + \dots + r_{i,t_i}s_{i,t_i}$  mit  $t_i \geq 0, s_{i,1}, \dots, s_{i,t_i} \in S$  und  $r_{i,1}, \dots, r_{i,t_i} \in R$  schreiben. Für  $S' := \{s_{i,j} \mid i = 1, \dots, s, j = 1, \dots, t_i\}$  gilt dann  $m_i \in \langle S' \rangle$  für alle  $i = 1, \dots, s$  und deshalb

$$M = \langle m_1, \dots, m_s \rangle \subseteq \langle S' \rangle \subseteq M.$$

Also ist  $\langle S' \rangle = M$  und somit  $S'$  ein endliches Erzeugendensystem von  $M$ .

#### Übung 32.

Es sei  $0 \rightarrow N \xrightarrow{f} M \xrightarrow{g} P \rightarrow 0$  eine kurze exakte Sequenz von  $R$ -Moduln.

1. Zeigen Sie, dass  $P$  endlich erzeugt ist, wenn  $M$  endlich erzeugt ist.

2. Zeigen Sie, dass  $M$  endlich erzeugt ist, wenn  $P$  und  $N$  endlich erzeugt sind.

**Übung 33. Charakterisierungen noetherscher Moduln**

Es sei  $M$  ein  $R$ -Modul. Zeigen Sie, dass die folgenden Bedingungen äquivalent sind:

1. Jeder  $R$ -Untermodul von  $M$  ist endlich erzeugt.
2. Jede aufsteigende Kette

$$N_0 \subseteq N_1 \subseteq N_2 \subseteq N_3 \subseteq N_4 \subseteq \dots$$

von  $R$ -Moduln stabilisiert, i.e. es gibt ein  $i \geq 0$  mit  $N_j = N_i$  für alle  $j \geq i$ .

3. Jede nicht-leere Menge  $\mathcal{S}$  bestehend aus  $R$ -Untermoduln von  $M$  besitzt ein (bezüglich der Inklusion) maximales Element.

**Übung 34.**

1. Geben Sie für einen passenden Ring  $R$  eine kurze exakte Sequenz  $0 \rightarrow N \rightarrow M \rightarrow P \rightarrow 0$  von  $R$ -Moduln an, die nicht spaltet.
2. Es sei  $R$  ein kommutativer Ring und  $F$  ein freier  $R$ -Modul. Zeigen Sie, dass jede kurze exakte Sequenz von  $R$ -Moduln  $0 \rightarrow N \rightarrow M \rightarrow F \rightarrow 0$  spaltet.

**Übung 35.**

Es sei  $R$  ein kommutativer Ring und  $I, J \subseteq R$  zwei Ideale, so dass  $R/I \cong R/J$  als  $R$ -Moduln. Zeigen Sie, dass bereits  $I = J$ . (Hinweis: Betrachten Sie Annihilatoren.)

**Lösung 35.**

Für jedes Ideal  $K \subseteq R$  gilt  $\text{Ann}(R/K) = K$ , weshalb  $I = \text{Ann}(R/I) = \text{Ann}(R/J) = J$  gilt.

**Übung 36. Torsionsuntermoduln**

Es sei  $R$  ein Integritätsbereich.

1. Definieren Sie den Torsionsuntermodul  $T(M)$  eines  $R$ -Moduls  $M$ , und zeigen Sie, dass es sich um einen  $R$ -Untermodul von  $M$  handelt.
2. Zeigen Sie, dass  $T(M \oplus N) = T(M) \oplus T(N)$  für alle  $R$ -Moduln  $M$  und  $N$ .
3. Zeigen Sie, dass jeder freie  $R$ -Modul torsionsfrei ist.
4. Zeigen Sie für jeden  $R$ -Moduln  $M$ , dass  $M/T(M)$  torsionsfrei ist.
5. Es sei  $f: M \rightarrow N$  ein  $R$ -Modulhomomorphismus. Zeigen Sie, dass  $f(T(M)) \subseteq T(N)$ .

Wir bezeichnen die Einschränkung von  $f: M \rightarrow N$  auf die entsprechenden Torsionsuntermoduln mit  $T(f): T(M) \rightarrow T(N)$ ,  $m \mapsto f(m)$ .

6. Zeigen Sie, dass

a)  $T(\text{id}_M) = \text{id}_{T(M)}$  für jeden  $R$ -Modul  $M$ , und

b)  $T(g \circ f) = T(g) \circ T(f)$  für alle  $R$ -Modulhomomorphismen  $N \xrightarrow{f} M \xrightarrow{g} P$ .

7. Zeigen Sie für jede exakte Sequenz von  $R$ -Moduln  $0 \rightarrow M \xrightarrow{f} N \xrightarrow{g} P \rightarrow 0$  die Exaktheit der Sequenz

$$0 \rightarrow T(M) \xrightarrow{T(f)} T(N) \xrightarrow{T(g)} T(P).$$

8. Zeigen Sie ferner, dass  $T(g)$  surjektiv ist, falls  $P$  projektiv ist.

9. Geben Sie ein Beispiel für einen surjektiven  $R$ -Modulhomomorphismus  $g: M \rightarrow P$  an, so dass  $T(g)$  nicht surjektiv ist.

### Übung 37.

Zeigen Sie, dass für jeden  $R$ -Moduln  $M$  die folgenden Bedingungen äquivalent sind:

1.  $M$  wird von einem einzelnen Element erzeugt, d.h. es gibt  $m \in M$  mit  $M = \langle m \rangle_R$ .
2. Es gilt  $M \cong R/\text{Ann}(M)$  als  $R$ -Moduln.
3. Es gibt ein Ideal  $I \subseteq R$  mit  $R/I \cong M$  als  $R$ -Moduln.

Erfüllt  $M$  eine (und damit alle) dieser Bedingungen, so heißt  $M$  *zyklisch*.

### Übung 38.

Ein  $R$ -Modul  $M$  heißt *einfach*, wenn  $M$  genau zwei Untermoduln hat.

1. Zeigen Sie, dass  $M$  genau dann einfach ist, wenn  $M \neq 0$  und  $0, M \subseteq M$  die einzigen beiden Untermoduln sind.
2. Zeigen Sie, dass für je zwei einfache  $R$ -Moduln  $M$  und  $N$  jeder  $R$ -Modulhomomorphismus  $f: M \rightarrow N$  entweder 0 oder ein Isomorphismus ist.

## 4 Körpertheorie

### Übung 39.

Zeigen Sie, dass für einen kommutativen Ring  $K$  die folgenden Bedingungen äquivalent sind:

1.  $K$  ist ein Körper.
2.  $K$  hat genau zwei Ideale.
3. Das Nullideal in  $K$  ist maximal.

### Lösung 39.

(1  $\implies$  2) Da  $K$  ein Körper ist gilt  $0 \neq K$ , also hat  $K$  mindestens zwei Ideale. Ist  $I \subseteq K$  ein Ideal mit  $I \neq 0$ , so gibt es ein  $x \in I$  mit  $x \neq 0$ . Dann ist  $x$  eine Einheit in  $K$ , somit  $K = (x) \subseteq I$  und deshalb  $I = K$ . Also sind  $0$  und  $K$  die einzigen Ideale in  $K$ .

(2  $\implies$  3) Es muss  $0 \neq K$ , denn sonst wäre  $0$  das einzige Ideal in  $K$ . Also sind  $0$  und  $K$  die einzigen beiden Ideale in  $K$ . Ist  $I \subseteq K$  ein Ideal mit  $0 \subsetneq I$ , so muss bereits  $I = K$ . Also ist  $0$  ein maximales Ideal.

(3  $\implies$  1) Da  $0 \subseteq K$  maximal ist, ergibt sich, dass  $K \cong K/0$  ein Körper ist.

### Übung 40.

Es sei  $K$  ein algebraisch abgeschlossener Körper. Zeigen Sie, dass  $K$  unendlich ist.

### Lösung 40.

Wäre  $K$  endlich, so wäre

$$p(T) := 1 + \prod_{\lambda \in K} (T - \lambda) \in K[T]$$

ein Polynom positiven Grades ohne Nullstellen (denn  $p(x) = 1$  für alle  $x \in K$ ). Dies stünde im Widerspruch zur algebraischen Abgeschlossenheit von  $K$ .