Übungen zu Einführung in die Algebra

Jendrik Stelzner

25. Januar 2017

Inhaltsverzeichnis

1 Ringtheorie

Übung 1. *Initialobjekte in der Kategorie der Ringe*

1. Überzeugen Sie sich davon, dass es für jeden Ring R genau einen Ringhomomorphismus $\mathbb{Z} \to R$ 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 $Z \to R$ gibt. Zeigen Sie, dass $Z \cong \mathbb{Z}$.

Lösung 1.

1. Ist $\phi\colon \mathbb{Z} \to R$ 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 ϕ eindeutig. Durch direktes Nachrechnen ergibt sich auch, dass $\psi\colon \mathbb{Z} \to R$ mit
$$\psi(n) := n \cdot 1_R \quad \text{für alle } n \in \mathbb{Z}$$
ein Ringhomomorphismus ist.

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

Übung 2.

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

Lösung 2.

Aus der Vorlesung ist bekannt, dass die Abbildung
$$\{\text{Ringhomomorphismen } \mathbb{Z}[T] \to R\} \to \{\text{Ringhomomorphismen } \mathbb{Z} \to R\} \times R,$$
$$\phi \mapsto (\phi|_{\mathbb{Z}}, \phi(T))$$
eine Bijektion ist. Da es genau einen Ringhomomorphismus $\mathbb{Z} \to R$ gibt, ergibt sich ferner, dass die Abbildung
$$\{\text{Ringhomomorphismen } \mathbb{Z} \to R\} \times R \to R, \quad (\psi, r) \mapsto r$$
eine Bijektion ist. Damit ergibt sich insgesamt eine Bijektion
$$\{\text{Ringhomomorphismen } \mathbb{Z}[T] \to R\} \to R, \quad \phi \mapsto \phi(T).$$

Übung 3.
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 3.
Dies ist eine Standardaussage, deren Beweis sich in jedem Algebra-Buch findet.

Übung 4.
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 $I = \sqrt{J}$ 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 4.

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 $k = 0, \ldots, n+m$ 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

$$\text{es gibt } n \in \mathbb{N} \text{ mit } \overline{x}^n = 0 \implies \overline{x} = 0 \qquad \text{für alle } x \in R. \tag{1}$$

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

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

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

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

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 Integritatsbereich, 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 5.

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 $\phi\colon R \to K$ mit $\ker \phi = \mathfrak{p}$ gibt.

Lösung 5.

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

$$\phi\colon R \xrightarrow{\pi} R/\mathfrak{p} \to Q(R/\mathfrak{p}),$$

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

Gibt es andererseits einen Körper K und einen Ringhomomorphismus $\phi\colon R \to K$ mit $\mathfrak{p} = \ker \phi$, so ist $R/\mathfrak{p} \cong \operatorname{im} \phi \subseteq K$. Der Körper K ist insbesondere ein Integritätsbereich, weshalb auch der Unterring $\operatorname{im}\phi$ ein Integritätsbereich ist. Der Quotient $R/\mathfrak{p}$ ist also ein Integritätsbereich und $\mathfrak{p}$ somit eine Primideal.

Übung 6.
Es sei K ein Körper.

1. Zeigen Sie, dass es für jedes Polynom $f \in K[X]$ einen eindeutigen K-linearen Ringhomomorphismus $\phi_f \colon K[X] \to K[X]$ gibt, so dass $\phi_f(X) = f$.

   (*Hinweis*: Zeigen Sie zunächst, dass $\phi_f|_K = \mathrm{id}_K$ gilt.)

2. Zeigen Sie, dass ϕ_f genau dann ein Ringisomorphismus ist, wenn $\deg f = 1$.

Übung 7. *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 $\phi \colon R \to S$ ein Ringhomomorphismus, so induziert ϕ per Einschränkung einen Gruppenhomomorphismus

$$\phi^\times \colon R^\times \to S^\times, \quad x \mapsto \phi(x).$$

3. Für jeden Ring kommutativen R gilt $\mathrm{id}_R^\times = \mathrm{id}_{R^\times}$, und für alle kommutativen Ringe R_1, R_2 und R_3 und Ringhomomorphismen $\phi \colon R_1 \to R_2$ und $\psi \colon R_2 \to R_3$ gilt $(\psi\phi)^\times = \psi^\times\phi^\times$.

4. Ist R ein kommutativer Ring und $\phi \colon R \to S$ ein Isomorphismus von Ringen, so ist $\phi^\times \colon R^\times \to S^\times$ 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 7.

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 ϕ mulitplikativ ist, gilt dies auch für $\phi^\times$, weshalb $\phi^\times$ ein Gruppenhomomorphismus ist.

3. Da $\mathrm{id}_R^\times(x) = \mathrm{id}_R(x) = x = \mathrm{id}_{R^\times}(x)$ für alle $x \in X$ gilt, ist $\mathrm{id}_R^\times = \mathrm{id}_{R^\times}$. 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 $\psi \coloneqq \phi^{-1} \colon S \to R$. Es gilt
$$\phi^\times \psi^\times = (\phi\psi)^\times = \left(\phi\phi^{-1}\right)^\times = \mathrm{id}_S^\times = \mathrm{id}_{S^\times}$$
und analog auch $\psi^\times \phi^\times = \mathrm{id}_{R^\times}$. Also ist der Gruppenhomomorphismus $\phi^\times$ bijektiv mit $(\phi^\times)^{-1} = (\phi^{-1})^\times$, und somit ein Gruppenisomorphismus.

Übung 8. *Urbilder von Idealen*

Es seien R und S zwei kommutative Ringe und $\phi \colon R \to S$ 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 8.

1. Es sei $\pi \colon S \to S/\mathfrak{a}$, $s \mapsto \overline{s}$ 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 $\pi \colon S \to S/\mathfrak{p}$, $s \mapsto \overline{s}$ die kanonische Projektion und $\mathfrak{q} \coloneqq \phi^{-1}(\mathfrak{p})$. 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
$$\psi \colon R/\mathfrak{q} \to S/\mathfrak{p} \quad \overline{r} \mapsto \overline{\phi(r)}.$$
Der Ring $\mathrm{im}(\pi\phi) \subseteq S/\mathfrak{p}$ ist als Unterring eines Integritätsbereichs ebenfalls ein Integritätsbereich. Somit ist $R/\mathfrak{q} \cong \mathrm{im}(\pi\phi)$ ein Integritätsbereich, also $\mathfrak{q}$ ein Primideal.

3. Die Aussage gilt nicht: Es sei etwa $\phi \colon \mathbb{Z} \to \mathbb{Q}$ die kanonische Inklusion. Dann ist $\mathfrak{m} \coloneqq 0$ 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 9.

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 9.
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 10. *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 10.
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 11.
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 11.
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 ε_1 eine Einheit mit $\varepsilon_1^{-1} = \varepsilon_2$. Da $y = \varepsilon_1 x$ ist $x \sim y$.

Übung 12.
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 13.
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 14.
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 15.
Es sei R ein euklidischer Ring. Zeigen Sie, dass R ein Hauptidealring ist.

Lösung 15.
Als euklidischer Ring ist R insbesondere ein Integritätsbereich. Es sei $g\colon R \to \mathbb{N}$ 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 eintretten. Also ist $r = 0$ und somit $x = ab \in (a)$.

Übung 16.
Es sei K ein kommutativer Ring, so dass $K[X]$ ein Hauptidealring ist. Zeigen Sie, dass K bereits ein Körper ist.

Lösung 16.
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
$$(a, X) = (f). \tag{3}$$
Wegen Gleichung (3) gilt $f \mid a$, d.h. es gibt $g \in K[X]$ mit $fg = a$. Entscheident ist nun die folgende Beobachtung:
Behauptung 1. Die übliche Gradabbildung $\deg\colon K[X] \to \mathbb{N}$ ist additiv.

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

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 $f = f_0 = a_0 p_0 = a p_0$. Deshalb gilt bereits $f = a p_0 \in (a)$. 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 $h(X) = b_1 X + b_0$ für $b_1, b_0 \in K$. Durch Koeffizientenvergleich erhalten wir aus der Gleichung
$$X = ah(X) = a(b_1 X + b_0) = ab_1 X + ab_0,$$
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. Ansonsonsten 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 17.
Es sei K ein Körper. Zeigen Sie, dass es in $K[X]$ unendlich viele irreduzible, normierte Polynome gibt.

Übung 18.
Es seien R und R' zwei kommutative Ringe, $S \subseteq R$ eine multiplikative Teilmenge und $f\colon R \to R'$ ein Ringhomomorphismus.

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

Lösung 18.
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 $i\colon R \to R_S, r \mapsto r/1$ und $i'\colon R' \to R'_{S'}, r' \mapsto r'/1$ die kanonischen Ringhomomorphismen. Die Komposition $i' \circ f\colon R \mapsto R'_{S'}$ 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 $f_S\colon R_S \to R'_{S'}$ mit $f_S i = i' f$, d.h. so dass das folgende Diagram kommutiert:
$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "i"] & R' \arrow[d, "i'"] \\ R_S \arrow[r, "f_S"] & R'_{S'} \end{tikzcd}$$

Übung 19.
Es sei R ein kommutativer Ring.

1. Zeigen Sie, dass für jedes Ideal $\mathfrak{a} \subseteq R$ die Teilmenge
$$\mathfrak{a}[X] := \left\{ \sum_i f_i X^i \in R[X] \,\middle|\, f_i \in \mathfrak{a} \text{ für alle } i \right\}$$
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 19.

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

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

Für $f = \sum_i f_i X^i \in R[X]$ ist genau dann $f \in \ker \varphi$, wenn $\overline{f_i} = 0$ 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 π und φ wie zuvor. Wegen der Surjektivität von π ist auch φ surjektiv. Somit induziert φ einen Ringisomorphismus

$$\psi \colon R[X]/\mathfrak{p}[X] \to (R/\mathfrak{p})[X], \quad \overline{\sum_i f_i X^i} \mapsto \sum_i \overline{f_i} X^i.$$

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 20).

Übung 20.
Zeigen Sie, dass es keinen Ring R gibt, so dass $R[X]$ ein Körper ist.

Lösung 20.
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 21.
Zeigen Sie, dass $\mathbb{Z}[i] \cong \mathbb{Z}[X]/(X^2 + 1)$.

Übung 22.
Es sei R ein kommutativer Ring und $f \in R$. Zeigen Sie, dass $R_f \cong R[X]/(fX-1)$.

Lösung 22.
Das Element $\overline{f} \in R[X]/(fX-1)$ ist eine Einheit mit $\overline{f}^{-1} = \overline{X}$ da

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

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

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

Andererseits induziert der kanonische Ringhomomorphismus $i\colon R \to R_f$, $r \mapsto r/1$ nach der universellen Eigenschaft des Polynomrings $R[X]$ einen eindeutigen Ringhomomorphismus $\tilde{\psi}\colon R[X] \to R_f$ 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 $\psi\colon R[X]/(fX-1) \to R_f$ mit $\psi(\overline{p}) = \tilde{\psi}(p)$ für alle $p \in R[X]$, d.h. es ist

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

Die beiden Ringhomomorphismen φ und ψ 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 φ ein Isomorphismus mit $\varphi^{-1} = \psi$.

Übung 23.
Bestimmen Sie die Einheitengruppe $\mathbb{Z}[i]^\times$.

Lösung 23.
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

$$1 = |1|^2 = |zz^{-1}|^2 = |z|^2|z^{-1}|. \tag{4}$$

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 24.
Formulieren und beweisen Sie den Hilbertschen Basissatz.

2 Modultheorie

Übung 25.
Zeigen Sie, dass es auf jeder abelschen Gruppe genau eine $\mathbb{Z}$-Modulstruktur gibt.

Lösung 25.
Es sei A eine abelsche Gruppe. Aus der Vorlesung ist die Bijektion

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

bekannt. Dabei ist

$$\operatorname{End}(A) = \{f \colon A \to A \mid f \text{ ist additiv}\}$$

ein Ring unter punktweiser Adddition und Komposition. Da es genau einen Ringhomomorphismus $\mathbb{Z} \to \operatorname{End}(A)$ gibt (siehe Übung 1) folgt die Aussage.

Übung 26.
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 $\lambda_s \colon M \to M$, $m \mapsto sm$ bijektiv ist.

Übung 27.
Es sei M ein endlich erzeugter R-Modul. Zeigen Sie, dass jedes Erzeugendensystem $S \subseteq M$ ein endliches Erzeugendensystem enthält.

Lösung 27.
Es sei $\{m_1, \dots, m_s\} \subseteq M$ ein endliches Erzeugendensystem. Da S ein Erzeugendensystem ist, lässt sich jedes m_i als $m_i = r_{i,1}s_{i,1} + \cdots + r_{i,t_i}s_{i,t_i}$ 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 28.
Es sei $0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0$ 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 29. *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 Untermoduln von M 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 30.

1. Geben Sie für einen passenden Ring R eine kurze exakte Sequenz $0 \to N \to M \to P \to 0$ 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 $0 \to N \to M \to F \to 0$ spaltet.

Übung 31.
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 31.
Für jedes Ideal $K \subseteq R$ gilt $\operatorname{Ann}(R/K) = K$, weshalb $I = \operatorname{Ann}(R/I) = \operatorname{Ann}(R/J) = J$ gilt.

Übung 32. *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 $f\colon M \to N$ ein R-Modulhomomorphismus. Zeigen Sie, dass $f(T(M)) \subseteq T(N)$.

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

6. Zeigen Sie, dass
   a) $T(\mathrm{id}_M) = \mathrm{id}_{T(M)}$ 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 $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ die Exaktheit der Sequenz
$$0 \to T(M) \xrightarrow{T(f)} T(N) \xrightarrow{T(g)} T(P).$$
8. Zeigen Sie ferner, dass $T(g)$ surjektiv ist, falls P projektiv ist.
9. Geben Sie ein Beispiel für einen surjektiven R-Modulhomomorphismus $g\colon M \to P$ an, so dass $T(g)$ nicht surjektiv ist.

Übung 33.
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 $M \cong R/\mathrm{Ann}(M)$ 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 34.
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 $f\colon M \to N$ entweder 0 oder ein Isomorphismus ist.

Übung 35.
Ein R-Modul M heißt *unzerlegbar*, falls es keine Zerlegung $M = N_1 \oplus N_2$ in zwei echten Untermoduln $N_1, N_2 \subsetneq M$ gibt.

1. Es sei R ein Integritätsbereich. Zeigen Sie, dass R als R-Modul unzerlegbar ist.
2. Geben Sie ein Beispiel für einen Ring R, der zwar nicht nullteilerfrei ist, so dass aber R als R-Modul dennoch unzerlegbar ist.
3. Geben Sie ein Beispiel für einen Ring R, so dass R als R-Modul nicht unzerlegbar ist.

3 Gruppentheorie

Übung 36. *Ein Kriterium für maximale Untergruppen*
Es sei G ein 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 36.
Es sei $p \coloneqq [G : H]$. Da p eine Primzahl ist gilt inbesondere $p \neq 1$, 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 $H = \langle (1\,2) \rangle = \{\mathrm{id}, (1\,2)\}$ ist H zwar nicht normal in G, aber $[G : H] = |G|/|H| = 6/2 = 3$ ist prim.

4 Körpertheorie

Übung 37.
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 37.
(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 38.
Es sei K ein algebraisch abgeschlossener Körper. Zeigen Sie, dass K unendlich ist.

Lösung 38.
Wäre K endlich, so wäre

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

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

Übung 39.
Es seien $p, q \in K[T]$ zwei normierte irreduzible Polynome mit $p \neq q$. Zeigen Sie, dass p und q in $\overline{K}$ keine gemeinsamen Nullstellen haben.

Lösung 39.
Gebe es eine gemeinsame Nullstelle $\alpha \in \overline{K}$ von p und q, so wären p und q beide das Minimalpolynom von α über K, und somit $p = q$.

Übung 40.
Es sei $K(\alpha)/K$ eine endliche, zyklische Körpererweiterung von ungeraden Grad. Zeigen Sie, dass $K(\alpha) = K(\alpha^2)$.

Lösung 40.
Da $K(\alpha^2) \subseteq K(\alpha)$ gilt, genügt es zu zeigen, dass $\alpha^2 \in K(\alpha)$. Wir nehmen an, dass $\alpha^2 \notin K(\alpha)$. Dann ist das normierte quadratische Polynom $P(T) \coloneqq T^2 - \alpha^2 \in K(\alpha^2)[T]$ irreduzibel mit $P(\alpha) = 0$, und deshalb das Minimalpolynom von α über $K(\alpha^2)$. Es ist also $[K(\alpha) : K(\alpha^2)] = 2$. Damit gilt

$$[K(\alpha) : K] = [K(\alpha) : K(\alpha^2)][K(\alpha^2) : K] = 2[K(\alpha^2) : K],$$

was im Widerspruch dazu steht, dass $[K(\alpha) : K]$ ungerade ist.