Übungen zu Einführung in die Algebra

Jendrik Stelzner

26. 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 $\mathbb{Z}$ 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 $\mathrm{id}_{\mathbb{Z}}\colon \mathbb{Z} \to \mathbb{Z}$ ist ebenfalls ein Ringhomomorphismus2. 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 gilt $\psi \circ \phi = \mathrm{id}_{\mathbb{Z}}$. Analog ergibt sich, dass auch $\phi \circ \psi = \mathrm{id}_Z$ gilt.

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.

1. Für alle $x \in R$ sei $\overline{x} \in R/\mathfrak{p}$ die entsprechende Äquivalenzklasse. Das Ideal $\mathfrak{p}$ ist genau dann prim, wenn die Aussage

$$\forall x, y \in R : \overline{x} \cdot \overline{y} = 0 \implies \overline{x} = 0 \text{ oder } \overline{y} = 0 \tag{1}$$

gilt. Da $\overline{x} \cdot \overline{y} = \overline{xy}$ für alle $x, y \in R$ gilt, ist die Aussage (1) äquivalent dazu, dass

$$\forall x, y \in R : \overline{xy} = 0 \implies \overline{x} = 0 \text{ oder } \overline{y} = 0. \tag{2}$$

Für alle $x \in R$ gilt genau dann $\overline{x} = 0$, wenn $x \in \mathfrak{p}$. Deshalb ist die Aussage (2) äquivalent dazu, dass

$$\forall x, y \in R : xy \in \mathfrak{p} \implies x \in \mathfrak{p} \text{ oder } y \in \mathfrak{p}. \tag{3}$$

Dies ist genau die Aussage, dass $\mathfrak{p}$ ein Primideal ist.

2. Es sei $\pi\colon R \to R/\mathfrak{m}$, $x \mapsto \overline{x}$ die kanonische Projektion. Wie aus der Vorlesung bekannt ist die Abbildung

$$\{\text{Ideale } I \subseteq R/\mathfrak{m}\} \to \{\text{Ideale } J \subseteq R \text{ mit } J \supseteq \mathfrak{m}\}, \quad I \mapsto \pi^{-1}(I)$$

eine wohldefinierte Bijektion. Der Ring $R/\mathfrak{m}$ ist genau dann ein Körper, wenn $R/\mathfrak{m}$ genau zwei Ideale enthält (man siehe Übung 40); das Ideal $\mathfrak{m}$ ist genau dann ein maximales Ideal in R, wenn es genau zwei Ideale $J \subseteq R$ mit $J \supseteq \mathfrak{m}$ gibt. Wegen der Existenz der obigen Bijektion sind beide Aussagen äquivalent.

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

$$\text{es gibt } n \in \mathbb{N} \text{ mit } \overline{x}^n = 0 \implies \overline{x} = 0 \qquad \text{für alle } x \in R. \tag{4}$$

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 (4) äquivalent dazu, dass

$$\text{es gibt } n \in \mathbb{N} \text{ mit } x^n \in I \implies x \in I \qquad \text{für alle } x \in R. \tag{5}$$

Durch Einsetzen der Definition von $\sqrt{I}$ ergibt sich aus (5) 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. *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 6.

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 7. *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 7.

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 $\mathfrak{m} := 0$ 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 8. *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 8.

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 9.

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 9.

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 10.
Es sei R ein kommutativer Ring.

1. Zeigen Sie, dass für nilpotentes $n \in R$ das Element $1 - n$ eine Einheit ist, und geben Sie $(1-n)^{-1}$ an.
2. Zeigen Sie, dass für nilpotentes $n \in R$ das Element $1 + n$ eine Einheit ist, und geben Sie $(1+n)^{-1}$ an.
3. Zeigen Sie, dass für nilpotentes $n \in R$ und jede Einheit $e \in R^\times$ das Element $e + n$ eine Einheit ist, und geben Sie $(e+n)^{-1}$ an.

Lösung 10.

1. Für $k \geq 0$ mit $n^k = 0$ gilt $(1-n)(1+n+\dots+n^{k-1}) = 1 - n^k = 1$. Also ist $1 - n$ eine Einheit mit $(1-n)^{-1} = \sum_{p=0}^{k-1} n^p = \sum_{p=0}^{\infty} n^p$.
2. Da n nilpotent ist, gilt dies auch für $-n$. Nach dem vorherigen Aufgabenteil ist deshalb $1 + n = 1 - (-n)$ eine Einheit mit $(1+n)^{-1} = (1-(-n))^{-1} = \sum_{p=0}^{\infty} (-1)^p n^p$.
3. Es gilt $e + n = e(1 + e^{-1}n)$, und da n nilpotent ist, gilt dies auch für $e^{-1}n$. Nach dem vorherigen Teil ist $1 + e^{-1}n$ eine Einheit, und somit $e + n$ als Produkt zweier Einheiten ebenfalls eine Einheit; ferner gilt
$$(e+n)^{-1} = e^{-1}(1+e^{-1}n)^{-1} = e^{-1} \sum_{p=0}^{\infty} (-1)^p (e^{-1}n)^p = \sum_{p=0}^{\infty} (-1)^p e^{-1-p} n^p.$$

Übung 11.
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 12.
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 13.
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 14.
Es sei R ein euklidischer Ring. Zeigen Sie, dass R ein Hauptidealring ist.

Lösung 14.
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 15.
Es sei K ein kommutativer Ring, so dass $K[X]$ ein Hauptidealring ist. Zeigen Sie, dass K bereits ein Körper ist.

Lösung 15.
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
$$(a, X) = (f). \tag{6}$$
Wegen Gleichung (6) 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 16. *Euklid*

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

Lösung 16.

Wir nehmen an, dass es nur endlich viele normierte, irreduzible Polynome in $K[X]$ gibt, nämlich $p_1, \ldots, p_n \in K[X]$. Man bemerke, dass $n \geq 1$, da die Polynome $X - a$ für $a \in K$ irreduzibel und normiert sind. Für das Element

$$q := 1 + p_1 \cdots p_n \in K[X]$$

gilt dann $\deg q \geq n \geq 1$. Es gilt $q \equiv 1 \pmod{p_i}$ für alle $i = 1, \ldots, n$, und somit $p_i \nmid q$ für alle $i = 1, \ldots, n$. Da die p_i ein Repräsentantensystem der Primelemente von $K[X]$ sind, widerspricht dies der Existenz einer Primfaktorzerlegung von q.

Übung 17.

Es sei R ein Ring und $I \subseteq R$ ein echtes Ideal. Zeigen Sie, dass es ein maximales Ideal $\mathfrak{m} \subseteq R$ gibt, so dass $I \subseteq \mathfrak{m}$.

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 $s_1's_2' = f(s_1)f(s_2) = f(s_1s_2) \in f(S) = S'$.
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

$$1 = |1|^2 = |zz^{-1}|^2 = |z|^2 |z^{-1}|. \tag{7}$$

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 (7) 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.

Übung 25. *Multiple Choice*
Entscheiden Sie, welche der folgenden Aussagen wahr oder falsch sind.

1. Jeder faktorielle Ring ist unendlich.

Lösung 25.

1. Die Aussage ist falsch. Jeder Körper ist ein faktorieller Ring, aber es gibt endliche Körper.

2 Modultheorie

Übung 26.
Zeigen Sie, dass es auf jeder abelschen Gruppe genau eine $\mathbb{Z}$-Modulstruktur gibt.

Lösung 26.
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 27.
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 28.
Es sei M ein endlich erzeugter R-Modul. Zeigen Sie, dass jedes Erzeugendensystem $S \subseteq M$ ein endliches Erzeugendensystem enthält.

Lösung 28.
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 $S' \coloneqq \{s_{i,j} \mid i = 1, \dots, s, j = 1, \dots, t_i\}$ 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 29.
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.

Lösung 29.

1. Es seien $m_1, \dots, m_t \in M$ mit $M = \langle m_1, \dots, m_t \rangle_R$. Wegen der Surjektivität von g gilt dann
$$P = g(M) = g(\langle m_1, \dots, m_t \rangle_R) = \langle g(m_1), \dots, g(m_t) \rangle_R,$$
weshalb P endlich erzeugt ist.

2. Es seien $n_1, \dots, n_s \in N$ und $p_{s+1}, \dots, p_t \in P$ endliche Erzeugendensysteme. Für alle $i = 1, \dots, s$ sei $m_i := f(n_i) \in M$; wegen der Surjektivität gibt es für jedes $i = s+1, \dots, t$ ein $m_i \in M$ mit $g(m_i) = p_i$. Dann gilt $\langle m_1, \dots, m_s, m_{s+1}, \dots, m_t \rangle_R = M$:

   Für $m \in M$ ist $g(m) \in P$ und deshalb $g(m) = r_{s+1}p_{s+1} + \dots + r_t p_t$ für passende $r_{s+1}, \dots, r_t \in R$. Es sei $m' := r_{s+1}m_{s+1} + \dots + r_t m_t \in M$. Es gilt
$$g(m') = r_{s+1}g(m_{s+1}) + \dots + r_t g(m_t) = r_{s+1}p_{s+1} + \dots + r_t p_t = g(m)$$
   und somit $m - m' \in \ker g = \operatorname{im} N$. Es sei $n \in N$ mit $f(n) = m - m'$. Dann gilt $n = r_1 n_1 + \dots + r_s n_s$ für passende $r_1, \dots, r_s \in R$, und somit
$$m - m' = f(n) = r_1 f(n_1) + \dots + r_s f(n_s) = r_1 m_1 + \dots + r_s m_s.$$
   Ingesamt erhalten wir, dass
$$m = m - m' + m' = r_1 m_1 + \dots + r_s m_s + r_{s+1}m_{s+1} + \dots + r_t m_t.$$

Übung 30.

Es sei R ein Hauptidealring und M ein endlich erzeugter R-Modul. Zeigen Sie, dass auch jeder Untermodul $N \subseteq M$ endlich erzeugt ist.

Lösung 30.

Es sei $m_1, \dots, m_t \in M$ ein endliches Erzeugendensystem und $\varphi\colon R^t \to M$ der eindeutige Homomorphismus von R-Moduln mit $\varphi(e_i) = m_i$ für alle $i = 1, \dots, t$ (hier bezeichnet $e_1, \dots, e_t \in R^t$ die Standardbasis). Dann ist φ surjektiv, und deshalb $F := \varphi^{-1}(N)$ ein Untermodul von R^t, für den $\varphi(F) = N$ gilt. Der R-Modul R^t ist frei vom Rang t; da R ein Hauptidealring ist, folgt daraus, dass der Untermodul $F \subseteq R^t$ frei vom Rang $s \leq t$ ist. Insbesondere ist F endlich erzeugt. Somit ist auch $N = \varphi(F)$ endlich erzeugt.

Übung 31. *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 maximales Element, d.h. ein Element $N \in \mathcal{S}$, das in keinem anderen Element von $\mathcal{S}$ echt enthalten ist.

Lösung 31.

Der Vollständigkeit halber geben wir mehr Implikationen an, als notwendig sind.

(1 $\implies$ 2) Es sei

$$N_0 \subseteq N_1 \subseteq N_2 \subseteq N_3 \subseteq N_4 \subseteq \dots \tag{8}$$

eine aufsteigende Kette von Untermoduln von M. Dann ist $N := \bigcup_{i\geq 0} N_i$ ein Untermodul von M. Nach Annahme ist N endlich erzeugt; es sei $n_1, \dots, n_t \in N$ ein endliches Erzeugendensystem. Da $n_1, \dots, n_t \in N = \bigcup_{i\geq 0} N_i$ gibt es für jedes $j = 1, \dots, t$ ein $i_j \geq 0$ mit $n_j \in N_{i_j}$; da $N_i \subseteq N_{i+1}$ für alle $i \geq 0$ gibt es bereits ein $I \geq 0$ mit $n_1, \dots, n_t \subseteq N_I$. Damit gilt

$$N = \langle n_1, \dots, n_t \rangle_R \subseteq N_I \subseteq \bigcup_{i\geq 0} N_i = N$$

und deshalb bereits $N = N_I$. Für alle $i \geq I$ git dann $N = N_I \subseteq N_i \subseteq N$ und somit $N_i = N_I$. Also stabilisiert die Kette (8).

(2 $\implies$ 1) Es gebe einen Untermodul $N \subseteq M$, der nicht endlich erzeugt ist. Es gilt notwendigerweise $N \neq 0$. Wir konstruieren eine nicht-stabilisierende Kette

$$N_0 \subsetneq N_1 \subsetneq N_2 \subsetneq N_3 \subsetneq N_4 \subsetneq \dots \subsetneq N \subseteq M$$

von endlich erzeugten von N wie folgt: Wir beginnen mit $N_0 := 0$. Ist N_i definiert, so gilt $N_i \subsetneq N$, da N_i endlich erzeugt ist, N aber nicht. Es gibt also $f \in N$ mit $f \notin N_i$. Da N_i endlich erzeugt ist, gilt dies auch für $N_{i+1} := N_i + \langle f \rangle_R$, und nach Wahl von f gilt $N_i \subsetneq N_{i+1}$.

(2 $\implies$ 3) Es gebe eine nicht-leere Menge $\mathcal{S}$ von Untermoduln von M, die kein maximales Element besitzt. Dann gibt es für jedes $N \in \mathcal{S}$ ein $N' \in \mathcal{S}$ mit $N \subsetneq N'$. Ausgehend von einem beliebigen $N_0 \in \mathcal{S}$ erhalten wir somit eine Kette

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

von Untermoduln von M, die nicht stabilisiert.

(3 $\implies$ 2) Es sei

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

eine aufsteigende Kette von Untermoduln von M. Dann ist $\mathcal{S} := \{N_i \mid i \in I\}$ eine nicht-leere Menge von Untermoduln von M. Nach Annahme hat $\mathcal{S}$ ein maximales Element, d.h. es gibt ein $i \in I$ mit $N_i \subsetneq N_j$ für alle $j \geq 0$. Es muss also bereits $N_i = N_j$ für alle $j \geq i$ gelten, weshalb die Kette stabilisiert.

(3 $\implies$ 1) Es sei $N \subseteq M$ ein Untermodul von M und

$$\mathcal{S} = \{P \subseteq N \mid P \text{ ist ein endlich erzeugter Untermodul von } N\}.$$

Dann ist $\mathcal{S}$ eine nicht-leere ($0 \in \mathcal{S}$) Menge von Untermoduln von M, und besitzt daher nach Annahme ein maximales Element N'. Wäre $N' \subsetneq N$, so gebe es ein $f \in N$ mit $f \notin N'$.

Dann wäre aber $N'' := N' + \langle f \rangle_R$ ein endlich erzeugter Untermodul von N, also ein Element von $\mathcal{S}$, mit $N' \subsetneq N''$, was der Maximalität von N' widerspricht. Also muss bereits $N = N'$, und N somit endlich erzeugt sein.

Übung 32.

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 $0 \to N \xrightarrow{f} M \xrightarrow{g} F \to 0$ spaltet.

Lösung 32.

1. Wir betrachten die folgende kurze exakte Sequenz von $\mathbb{Z}$-Moduln, d.h. von abelschen Gruppen:
$$0 \to \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \xrightarrow{x \mapsto \overline{x}} \mathbb{Z}/2 \to 0$$
Würde diese kurze exakte Sequenz spalten, so wäre $\mathbb{Z} \cong \mathbb{Z} \oplus \mathbb{Z}/2$. Dies gilt aber nicht, wie man den folgenden Gründen entnehmen kann:
   - Dies würde dem Hauptsatz über endlich erzeugte abelsche Gruppen widersprechen.
   - $\mathbb{Z}/2$ wäre isomorph zu einer Untergruppe von $\mathbb{Z}$ und somit torsionsfrei (denn $\mathbb{Z}$ ist frei und somit auch torsionsfrei, und Untergruppen von torsionsfreien abelschen Gruppen sind ebenfalls torsionsfrei), aber $2 \cdot \mathbb{Z}/2 = 0$.
   - $\mathbb{Z}/2$ wäre isomorph zu einer Untergruppe von $\mathbb{Z}$, und müsste somit entweder trivial oder unendlich sein, was beides nicht gilt.

2. Es sei $(e_i)_{i \in I}$ eine Basis von F. Wegen der Surjektivität von g gibt es für jedes $i \in I$ ein $m_i \in M$ mit $g(m_i) = e_i$. Es sei $h \colon F \to M$ der eindeutige Homomorphismus von R-Moduln mit $h(e_i) = m_i$ für alle $i \in I$. Dann gilt $g(h(e_i)) = g(m_i) = e_i$ für alle $i \in I$, und wegen der R-Linearität von $g \circ h$ somit bereits $g(h(x)) = x$ für alle $x \in F$. Also ist $g \circ h = \mathrm{id}_F$, weshalb die gegebene kurze exakte Sequenz spaltet.

Übung 33.

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 33.

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

Übung 34. *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 35.
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*.

Lösung 35.
(1 $\implies$ 2) Es sei $m \in M$ mit $M = \langle m \rangle_R$. Dann gilt
$$\mathrm{Ann}(M) = \mathrm{Ann}(\langle m \rangle_R) = \mathrm{Ann}(m) = \{r \in R \mid rm = 0\}.$$
Für den surjektive Homomorphismus von R-Moduln
$$\varphi\colon R \to M, \quad r \mapsto rm$$
gilt deshalb $\ker \varphi = \mathrm{Ann}(M)$. Somit induziert φ einen Isomorphismus von R-Moduln
$$\bar{\varphi}\colon R/\operatorname{Ann}(M) \to M, \quad [r] \mapsto rm.$$

(2 $\implies$ 3) Man setze $I = \mathrm{Ann}(M)$.
(3 $\implies$ 1) Ist $\varphi\colon R/I \to M$ ein Isomorphismus, so gilt

$$M = \varphi(R/I) = \varphi(\langle \overline{1} \rangle_R) = \langle \varphi(\overline{1}) \rangle_R.$$

Übung 36. *Schurs Lemma*
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.

Lösung 36.

1. Ist M einfach, so muss $M \neq 0$, da M sonst nur einen Untermodul hätte (nämlich sich selbst). Dann sind $0, M \subseteq M$ zwei verschiedene Untermoduln, und nach Annahme gibt es keine weiteren Untermoduln.

   Ist $M \neq 0$ und sind $0, M \subseteq M$ die einzigen beiden Untermoduln, so hat M genau zwei Untermoduln.

2. Ist $f\colon M \to N$ ein Homomorphismus von R-Moduln mit $f \neq 0$, so sind $\ker f \subseteq M$ und $\operatorname{im} f \subseteq N$ Untermoduln mit $\ker f \neq M$ und $\operatorname{im} f \neq 0$. Ist M einfach, so muss bereits $\ker f = 0$ gelten, und f somit bereits injektiv sein. Ist N einfach, so muss bereits $\operatorname{im} f = N$ gelten, und f somit bereits surjektiv sein. Sind M und N beide einfach, so ist f also bereits ein Isomorphismus.

Bemerkung. Das Lemma von Schur besagt insbesondere, dass der Endomorphismenring eines einfachen Moduls ein Schiefkörper ist.

Übung 37.
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.

   (*Hinweis*: Zeigen Sie, dass $I \cap J \neq 0$ für alle Ideale $I, J \subseteq R$ mit $I, J \neq 0$.)

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 38.

1. Es sei G eine Gruppe und $H_1, H_2 \subseteq G$ seien zwei Untergruppen. Zeigen Sie, dass $H_1 \cup H_2$ genau dann eine Untergruppe ist, wenn $H_1 \subseteq H_2$ oder $H_2 \subseteq H_1$.

2. Geben Sie ein Beispiel für eine eine Gruppe G und Untergruppen $H_1, H_2, H_3 \subseteq G$ an, so dass zwar $H_i \subsetneq H_j$ für alle $i \neq j$, aber $H_1 \cup H_2 \cup H_3$ eine Untergruppe von G ist.

Lösung 38.

1. Gilt $H_1 \subseteq H_2$ oder $H_2 \subseteq H_1$, so gilt $H_1 \cup H_2 = H_2$ oder $H_1 \cup H_2 = H_1$, weshalb $H_1 \cup H_2$ dann eine Untergruppe ist.

   Gilt $H_1 \nsubseteq H_2$ und $H_2 \nsubseteq H_1$, so gibt es $h_1 \in H_1$ mit $h_1 \notin H_2$ und $h_2 \in H_2$ mit $h_2 \notin H_1$. Es ist $h_1 h_2 \notin H_1$, da sonst $h_2 = h_1^{-1} h_1 h_2 \in H_1$ gelten würde; analog gilt auch $h_1 h_2 \notin H_2$. Insgesamt gilt somit $h_1 h_2 \notin H_1 \cup H_2$, obwohl $h_1, h_2 \in H_1 \cup H_2$. Also ist $H_1 \cup H_2$ nicht multiplikativ abgeschlossen, und somit keine Untergruppe von G.

2. Es sei $G = \mathbb{Z}/2 \oplus \mathbb{Z}/2$ und es seien

$$
\begin{aligned}
H_1 &= \langle (1,0) \rangle = \{(0,0), (1,0)\}, \\
H_2 &= \langle (1,1) \rangle = \{(0,0), (1,1)\}, \\
H_3 &= \langle (0,1) \rangle = \{(0,0), (0,1)\}.
\end{aligned}
$$

   Dann gilt $H_i \subseteq H_j$ für alle $1 \leq i \neq j \leq n$ und $H_1 \cup H_2 \cup H_3 = G$.

Übung 39. *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 39.

Es sei $p := [G : H]$. 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 40.
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 40.
($1 \implies 2$) 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 41.
Es sei K ein algebraisch abgeschlossener Körper. Zeigen Sie, dass K unendlich ist.

Lösung 41.
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 42.
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 42.
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 43.
Es sei $K(\alpha)/K$ eine endliche, zyklische Körpererweiterung von ungeraden Grad. Zeigen Sie, dass $K(\alpha) = K(\alpha^2)$.

Lösung 43.
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 $P(T) := T^2 - \alpha^2 \in K(\alpha^2)[T]$ 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.

Übung 44.
Es sei K ein algebraisch abgeschlossener Körper und L/K eine algebraische Körpererweiterung. Zeigen Sie, dass bereits $L = K$ gilt.

Lösung 44.
Es sei $\alpha \in L$. Da L/K algebraisch ist, gibt es ein normiertes Polynom $P \in K[T]$ mit $P \neq 0$ und $P(\alpha) = 0$. Da K algebraisch abgeschlossen ist zerfällt P in Linearfaktoren, also $P(T) = (T - a_1) \cdots (T - a_n)$ mit $a_1, \dots, a_n \in K$ und $n = \deg P$. Da

$$0 = P(\alpha) = (\alpha - a_1) \cdots (\alpha - a_n)$$

muss bereits $\alpha = a_i$ für ein $1 \leq i \leq n$, und somit $\alpha \in K$.

Übung 45.
Zeigen Sie, dass endliche Körpererweiterungen algebraisch sind.

Lösung 45.
Es sei L/K eine endliche Körpererweiterung und $x \in L$. Für den K-Untervektorraum $\langle \{x^n \mid n \in \mathbb{N}\} \rangle_K \subseteq L$ gilt

$$\dim_K \langle \{x^n \mid n \in \mathbb{N}\} \rangle_K \leq \dim_K L = [L : K] < \infty,$$

weshalb die Potenzen x^n mit $n \in \mathbb{N}$ linear abhängig über K sind. Also gibt es eine nichttriviale Linearkombination

$$a_n x^n + \cdots + a_1 x + a_0 = 0$$

mit $n \geq 1$ und $a_n, \dots, a_0 \in K$ mit $a_n \neq 0$. Für das Polynom

$$P(T) := a_n T^n + \cdots + a_1 T + a_0 \in K[T]$$

gilt also $P(x) = 0$, weshalb x algebraisch über K ist.

Übung 46.
Es sei L/K eine Körpererweiterung und es seien $\alpha, \beta \in L$. Zeigen Sie, dass α und β genau dann beide algebraisch über K sind, wenn $\alpha + \beta$ und $\alpha\beta$ beide algebraisch über K sind.

Bemerkung. Da π und e transzenent (über $\mathbb{Q}$) sind, muss $\pi + e$ oder $\pi \cdot e$ transzendent sein. Es ist nicht bekannt, welches von beiden.

Lösung 46.
Sind α und β algebraisch über K, so ist $K(\alpha, \beta)/K$ eine algebraische Körpererweiterung. Da $\alpha + \beta, \alpha\beta \in K(\alpha, \beta)$ sind $\alpha + \beta$ und $\alpha\beta$ dann algebraisch über K.

Es seien nun $\alpha + \beta$ und $\alpha\beta$ algebraisch über K. Dann ist $K(\alpha + \beta, \alpha\beta)/K$ eine algebraische Erweiterung. Auch die Erweiterung $K(\alpha, \beta)/K(\alpha + \beta, \alpha\beta)$ ist algebraisch, da α und β Nullstellen des Polynoms

$$P(T) \coloneqq (T - \alpha)(T - \beta) = T^2 - (\alpha + \beta)T + \alpha\beta \in K(\alpha + \beta, \alpha\beta)[T]$$

sind. Wegen der Transitivität von Algebraizität folgt, dass auch $K(\alpha, \beta)/K$ algebraisch ist, also α und β algebraisch über K sind.

Übung 47.
Es sei L/K eine Körpererweiterung, so dass $p \coloneqq [L : K]$ endlich und prim ist. Zeigen Sie, dass L/K ein zyklische Erweiterung ist, und bestimmen Sie alle $\alpha \in L$ mit $L = K(\alpha)$.

Lösung 47.
Für alle $\alpha \in K$ ist $K(\alpha) = K$. Ist $\alpha \in L$ mit $\alpha \notin K$, so ist $K(\alpha)/K$ eine echte Körpererweiterung, weshalb $[K(\alpha) : K] \neq 1$ gilt. Aus

$$p = [L : K] = [L : K(\alpha)] \underbrace{[K(\alpha) : K]}_{\neq 1}$$

folgt, da p prim ist, dass $[L : K(\alpha)] = 1$ (und $[K(\alpha) : K] = p$), und somit $K(\alpha) = L$. Also ist L eine zyklische Körpererweiterung, und die möglichen Elemente sind genau die $\alpha \in L$, für die $\alpha \notin K$.

Übung 48.
Es sei L/K eine endliche Körpererweiterung mit $[L : K] = 2^k$ für ein $k \geq 0$. Es sei $P \in K[T]$ ein kubisches Polynom, das eine Nullstelle in L hat. Zeigen Sie, dass f bereits eine Nullstelle in K hat.

Lösung 48.
Es sei $\alpha \in L$ eine Nullstelle von P. Wir können o.B.d.A. davon ausgehen, dass P normiert ist. Hätte P keine Nullstelle in K, so wäre P irreduzibel in $K[T]$, da P kubisch ist. Damit wäre dann P das Minimalpolynom von α über K, und somit $[K(\alpha) : K] = \deg P = 3$. Dann wäre aber

$$3 = [K(\alpha) : K] \mid [L : K(\alpha)][K(\alpha) : K] = [L : K] = 2^k,$$

was nicht gilt.

Übung 49.
Zeigen Sie, dass eine Körpererweiterung L/K genau dann algebraisch ist, wenn jeder Zwischenring $K \subseteq R \subseteq L$ bereits ein Körper ist.

Lösung 49.

Es sei L/K algebraisch und $K \subseteq R \subseteq L$ ein Zwischenring. Für $\alpha \in R$ ist dann α algebraisch über K, und somit $K(\alpha) = K[\alpha]$. Da R ein Ring ist, der α und R enthält, gilt $K[\alpha] \subseteq R$. Somit ist $K(\alpha) = K[\alpha] \subseteq R$. Ist $\alpha \neq 0$, so ist inbesondere $\alpha^{-1} \in K(\alpha) \subseteq R$. Das zeigt, dass jedes Element $\alpha \in R$ mit $\alpha \neq 0$ in R invertierbar ist. Somit ist R ein Körper. (Die Kommutativität von R ist klar, es sich um einen Unterring von L handelt, und L als Körper kommutativ ist.)

Es sei nun L/K nicht algebraisch. Dann gibt es ein Element $\alpha \in L$, das transzendent über K ist. Der Zwischenring $K \subseteq K[\alpha] \subseteq L$ ist dann kein Körper: Für den Polynomring $K[T]$ ist der Einsetzhomorphismus $K[T] \to K[\alpha]$, $P(T) \to P(\alpha)$ surjektiv, und wegen der Transzendenz von α auch injektiv, und somit ein Isomorphismus. Der Polynomring $K[T]$, und somit auch $K[\alpha]$, ist aber kein Körper.