Übungen zu Einführung in die Algebra

Jendrik Stelzner

12. Februar 2017

Inhaltsverzeichnis

1 Ringtheorie 2

2 Modultheorie 28

3 Gruppentheorie 48

4 Körpertheorie 52

1 Ringtheorie

Übung 1. *Multiple Choice*
Entscheiden Sie, welche der folgenden Aussagen wahr oder falsch sind.

1. Jeder Körper ist faktoriell.
2. Die beiden Projektionen $\pi_1, \pi_2 \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ mit $\pi_1(x, y) = x$ und $\pi_2(x, y) = y$ für alle $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ sind die einzigen beiden Ringhomomorphismen $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.
3. Für alle Ringe R_1 und R_2 gilt $(R_1 \times R_2)[X] \cong R_1[X] \times R_2[X]$.
4. Jeder faktorielle Ring ist unendlich.
5. Jeder endliche Integritätsbereich ist ein Hauptidealring.
6. Ist R ein endlicher kommutativer Ring, so ist $R[X, Y]$ noethersch.
7. Ist R ein Hauptidealring, so ist auch $R[X]$ ein Hauptidealring.
8. Ist R ein Integritätsbereich und $p \in R$ prim, so ist p irreduzibel.
9. Sind $n_1, n_2, n_3 \in \mathbb{Z}$ mit $\mathrm{ggT}(n_1, n_2, n_3) = 1$, so hat das Gleichungssystem
$$\begin{cases} x & \equiv & a_1 & \mod n_1, \\ x & \equiv & a_2 & \mod n_2, \\ x & \equiv & a_3 & \mod n_3, \end{cases}$$
für alle $a_1, a_2, a_3 \in \mathbb{Z}$ eine Lösung.
10. Ist R ein endlicher kommutativer Ring mit $p \coloneqq \operatorname{char} R > 0$ prim, so ist die Abbildung $R \to R$, $x \mapsto x^p$ ein Ringautomorphismus.

Lösung 1.
1. Die Aussage ist wahr:
2. Die Aussage ist wahr:
3. Die Aussage ist wahr: Die kanonischen Projektionen $\pi_i \colon R_1 \times R_2 \to R_i$, $(x_1, x_2) \mapsto x_i$ induzieren Ringhomomorphismen
$$\pi_i[X] \colon (R_1 \times R_2)[X] \to R_i[X], \quad \sum_j \left(x_j^{(1)}, x_j^{(2)}\right) X^j \mapsto \sum_j x_j^{(i)} X^j$$
die in einen Ringhomomorphismus
$$\varphi \colon (R_1 \times R_2)[X] \xrightarrow{\pi_1[X] \times \pi_2[X]} R_1[X] \times R_2[X],$$
$$\sum_j (a_j, b_j) X^j \mapsto \left(\sum_j a_j X^j, \sum_j b_j X^j \right)$$
resultieren. Die Bijektivität von φ ergibt sich durch direktes Hinsehen.

4. Die Aussage ist falsch: Jeder Körper ist ein faktorieller Ring, aber es gibt endliche Körper.
5. Die Aussage ist wahr: Jeder endliche Integritätsbereich ist bereits ein Körper.
6. Die Aussage ist wahr: R ist noethersch, und nach iterierter Anwendung des Hilbertschen Basissatzes somit auch $R[X][Y] \cong R[X,Y]$.
7. Die Aussage ist falsch: Ist K ein Körper, so ist zwar $R := K[X]$ ein Hauptidealring, aber $R[Y] \cong K[X,Y]$ nicht (siehe Übung 15). Allgemeiner ist $R[X]$ genau dann ein Hauptidealring, wenn R bereits ein Körper ist (siehe Übung 24).
8. Die Aussage ist wahr: Es seien $a, b \in R$ mit $p = ab$. Da p prim ist, gilt $p \mid a$ oder $p \mid b$; wir können o.B.d.A. davon ausgehen, dass $p \mid a$. Dann gibt es $c \in R$ mit $a = pc$ und es folgt $p = ab = pcb$. Da R ein Integritätsbereich ist, und $p \neq 0$ gilt (denn p ist prim) folgt, dass bereits $1 = cb$ gilt. Also ist b eine Einheit.
9. Die Aussage ist falsch:
10. Die Aussage ist falsch:

Übung 2.
Entscheiden Sie, ob die folgenden Polynome jeweils irreduzibel sind:

1. $f(X) := (X-3)^2 + 1 \in \mathbb{Q}[X]$.
2. $f(X) := 2X^3 - 14X + 2 \in \mathbb{Q}[X]$.
3. $f(X) := 2X^3 - 14X + 2 \in \mathbb{Z}[X]$.
4. $f(X) := X^3 - 18X^2 + 6X + 3 \in \mathbb{Q}[X]$.
5. $f(X) := X^3 - 18X^2 + 6X + 3 \in \mathbb{R}[X]$.
6. $f(X) := X^5 + 15X^2 + 6X + 21 \in \mathbb{Z}[X]$.
7. $f(X) := X^3 + 2X^2 + X + 1 \in \mathbb{Z}[X]$.
8. $f(X) := 2X^4 + 200X^3 + 2000X^2 + 20000X + 20 \in \mathbb{Q}[X]$.
9. $f(X) := X^n - 2t \in K(t)[X]$ für einen Körper K und $n \geq 1$.
10. $f(X,Y) := XY^3 + X^2Y + 5XY^2 + X^2 + 3XY + 2X + Y + 2 \in \mathbb{Q}[X]$.
11. $f(X,Y) := X^3 + Y^3 + X^2Y + XY^2 + XY + 6X + 6Y + 3 \in \mathbb{Q}[X,Y]$.
12. $f(X) := X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Q}[X]$ für $p > 0$ prim.
13. $f(X) := X^n + X^{n-1} + \cdots + X + 1 \in \mathbb{Q}[X]$ für $n \geq 3$ ungerade.

Lösung 2.

1. Wir geben zwei Möglichkeiten an, um die Irreduziblität von f zu zeigen:
   - Es handelt sich um ein quadratisches Polynom ohne reellen, und damit auch ohne rationale Nullstellen; also ist f irreduzibel.
   - Alternativ ergibt sich durch Ausmultiplizieren, dass $f(X) = X^2 - 6X + 10$, und die Irreduziblität von f ergibt sich aus Eisenstein mit $p = 2$.

2. Da $2 \in \mathbb{Q}$ eine Einheit ist, dürfen wir f durch 2 teilen und stattdessen das Polynom $\tilde{f}(X) = X^3 - 7X + 1 \in \mathbb{Q}[X]$ betrachten. Da es sich bei $\tilde{f}$ ein kubisches Polynom handelt, ist es genau dann irreduzibel, wenn es keine Nullstelle hat. Da $\tilde{f}$ normiert ist und bereits $\tilde{f} \in \mathbb{Z}[X]$ gilt, ist jede Nullstelle von $\tilde{f}$ schon eine ganze Zahl. Da jede Nullstelle $n \in \mathbb{Z}$ den konstanten Teil von $\tilde{f}$ teilen muss, kommen nur 1 und -1 als mögliche Nullstellen in Frage. Durch direktes Ausprobieren können aber beide ausgeschlossen werden. Also hat $\tilde{f}$ keine Nullstelle und ist somit irreduzibel.

3. Das Polynom ist nicht irreduzibel, da es in $f(X) = 2 \cdot (X^3 - 7X + 1)$ faktorisiert, wobei keiner der beiden Faktoren eine Einheit in $\mathbb{Z}[X]$ ist.

4. Reduzieren bezüglich $p = 3$ liefert $\tilde{f}(X) = X^3 - 4X - 1 = X^3 + 2X + 2 \in \mathbb{F}_3[X]$. Durch direktes Ausprobieren ergibt sich, dass $\tilde{f}$ keine Nullstellen hat, und als kubisches Polynom somit irreduzibel ist. Somit ist auch f irreduzibel.

5. Das Polynom ist nach Eisenstein mit $p = 3$ irreduzibel.

6. Das Polynom ist nicht irreduzibel, da es (als Polynom ungeraden Grades über $\mathbb{R}$) eine Nullstelle hat, aber nicht linear ist.

7. Die Irreduziblität ergibt sich nach Eisenstein mit $p = 3$.

8. Wir geben zwei Möglichkeit an die Irreduziblität von f zu zeigen.
   - Es genügt zu zeigen, dass f irreduzibel in $\mathbb{Q}[X]$ ist. Als kubisches Polynom ist f genau dann irreduzibel in $\mathbb{Q}[X]$, wenn es über $\mathbb{Q}$ keine Nullstelle hat. Da f normiert ist, muss jede rationale Nullstelle von f bereits eine ganze Zahl sein. Es genügt also zu zeigen, dass f keine ganzen Nullstellen hat. Jede ganze Nullstelle von f muss den konstanten Teil von f, also 1, teilen; es kommen somit nur 1 und -1 in Frage. Durch Ausprobieren ergibt sich, dass keines von beiden eine Nullstelle ist. Also ist f irreduzibel.
   - Reduzieren bezüglich $p = 2$ ergibt das Polynom $\tilde{f}(X) = X^3 + X + 1 \in \mathbb{F}_2[X]$. Dann hat $\tilde{f}$ keine Nullstellen und ist als kubisches Polynom deshalb irreduzibel. Somit ist auch f schon irreduzibel.

9. Da $2 \in \mathbb{Q}$ eine Einheit ist, dürfen wir f durch 2 teilen und somit stattdessen das Polynom $\tilde{f}(X) \coloneqq X^4 + 100X^3 + 1000X^2 + 10000X + 10 \in \mathbb{Q}[X]$ betrachten. Da $\tilde{f}$ normiert, und somit primitiv ist, ergibt sich die Irreduziblität von $\tilde{f}$ durch Eisenstein wahlweise mit $p = 2$ oder $p = 5$.

10. Die Irreduziblität ergibt sich durch Eisenstein mit dem Primelement $t \in K[t]$.

11. Wir betrachten das gegebene Polynom als

$$\begin{aligned}\tilde{f}(X) &= XY^3 + X^2Y + 3XY^2 + X^2 + 3XY + 2X + Y + 2 \\ &= (Y+1)X^2 + (Y^3 + 3Y^2 + 3Y + 2)X + (Y+2) \in \mathbb{Q}[Y][X]\end{aligned}$$

Da die Polynome $Y+1, Y+2 \in \mathbb{Q}[Y]$ teilerfremd sind, ist dieses Polynom primitiv. Außerdem gilt $(Y+2) \mid (Y^3+3Y^2+3Y+2)$, da -2 eine Nullstelle von Y^3+3Y^2+3Y+2 ist. Es lässt sich also Eisenstein mit dem Primelement $Y+2 \in \mathbb{Q}[Y]$ anwenden, um die Irreduziblität von $\tilde{f}$ zu erhalten.

12. Wir betrachen das gegeben Polynom als

$$\begin{aligned}\tilde{f}(Y) &= X^3 + Y^3 + X^2Y + XY^2 + XY + 6X + 6Y + 3 \\ &= Y^3 + XY^2 + (X^2 + X + 6)Y + (X^3 + 6X + 3) \in \mathbb{Q}[X][Y]\end{aligned}$$

Da $\tilde{f}$ normiert ist können wir bezüglich $X \in \mathbb{Q}[X]$ reduzieren, und erhalten

$$\overline{f}(Y) = Y^3 + 6Y + 3 \in (\mathbb{Q}[X]/(X))[Y] \cong \mathbb{Q}[Y].$$

Nach Eisenstein mit $p = 3$ ist $\overline{f}(Y)$ irreduzibel, also ist auch $\tilde{f}$, und somit f, irreduzibel.

13. Es gilt $f(X) = X^{p-1} + \cdots + X + 1 = (X^p - 1)/(X - 1)$ und somit

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

Dabei gilt $p \mid \binom{p}{k+1}$ für alle $k = 0, \ldots, p-1$ aber $p^2 \mid p = \binom{p}{1}$. Also ist das normierte Polynom $f(X+1)$ nach Eisenstein irreduzibel, und somit auch $f(X)$.

14. Das Polynom ist nicht linear, hat aber -1 ein Nullstelle; es ist also reduzibel.

Übung 3. *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 3.

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

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

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 Ringhomomorphismus. 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 4.
Es sei R ein Ring. Konstruieren Sie eine Bijektion zwischen der Menge der Ringhomomorphismen $\mathbb{Z}[T] \to R$ und R.

Lösung 4.
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 5. *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 5.
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 6.
Es sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal. Es sei $\pi\colon R \to R/I$, $x \mapsto \overline{x}$ die kanonische Projektion.

1. Zeigen Sie, dass
$$\begin{aligned}\{\text{Ideale } J \subseteq R \text{ mit } J \supseteq I\} &\longleftrightarrow \{\text{Ideale } K \subseteq R/I\},\\ J &\longmapsto \pi(J),\\ \pi^{-1}(K) &\longmapsfrom K\end{aligned}$$
eine wohldefinierte Bijektion liefert.

2. Zeigen Sie, dass sich die obige Bijektion sich zu Bijektion zwischen den jeweiligen Primidealen und maximalen Idealen einschränkt.

Lösung 6.
1. Für jedes Ideal $K \subseteq R/I$ ist das Urbild $\pi^{-1}(K) \subseteq R$ ebenfalls ein Ideal, denn Urbilder von Idealen unter Ringhomomorphismen sind ebenfalls Ideale (siehe Übung 5). Aus $0 \subseteq K$ ergibt sich, dass dabei $I = \ker \pi = \pi^{-1}(0) \subseteq \pi^{-1}(K)$.

   Wegen der Surjektivität von π ist für jedes Ideal $J \subseteq R$ auch $\pi(J) \subseteq R/I$ ein Ideal: Für $\overline{x}, \overline{y} \in \pi(J)$ kann $x, y \in J$ gewählt werden; dann ist auch $x + y \in J$ und somit $\overline{x} + \overline{y} = \overline{x + y} \in \pi(J)$. Für $\overline{x} \in \pi(J)$ und $\overline{r} \in R/I$ kann $x \in J$ gewählt werden; dann ist auch $rx \in J$ und somit $\overline{r}\overline{x} = \overline{rx} \in \pi(J)$.

   Das zeigt, dass die beiden Abbildungen wohldefiniert sind.

   Wegen der Surjektivität von π gilt $\pi(\pi^{-1}(K)) = K$ für jede Teilmenge $K \subseteq R/I$, inbesondere also für die Ideale.

   Für jedes Ideal $J \subseteq R$ gilt $\pi^{-1}(\pi(J)) = J + I$: Es gilt $J \subseteq \pi^{-1}(\pi(J)) \subseteq J$ und wie bereits gezeigt auch $I \subseteq \pi^{-1}(\pi(J))$, und somit $I + J \subseteq \pi^{-1}(\pi(J))$. Ist andererseits $x \in \pi^{-1}(\pi(J))$, so gibt es $d \in J$ mit $\overline{x} = \overline{y}$. Dann ist $\overline{x - y} = \overline{x} - \overline{y} = 0$, somit $x - y \in I$ und deshalb $x = (x - y) + y \in I + J$. Gilt bereits $I \subseteq J$, so ist $I + J = J$ und somit $\pi^{-1}(\pi(J)) = J$.

   Das zeigt, dass beide Abbildungen invers zueinander sind.

2. Wir bemerken zunächst, dass
$$\pi(J) = \{\overline{x} \mid x \in J\} = \{x + I \mid x \in J\} = J/I$$
für jedes Ideal $J \subseteq R$ mit $J \supseteq I$. Inbsbesondere gilt deshalb nach dem dritten Isomorphiesatz, dass $R/J \cong (R/I)/(J/I) \cong (R/I)/\pi(J)$. Es gilt somit
$$\begin{aligned}J \text{ ist prim} &\iff R/J \text{ ist ein Integritätsbereich}\\ &\iff (R/I)/\pi(J) \text{ ist ein Integritätsbereich} \iff \pi(J) \text{ ist prim.}\end{aligned}$$

Die Aussage für maximale Ideale ergibt sich analog, indem man *prim* durch *maximal* und *Integritätsbereich* durch *Körper* ersetzt.

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.

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. Wir erhalten eine wohldefinierte Bijektion

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

   (siehe Übung 6). Der Ring $R/\mathfrak{m}$ ist genau dann ein Körper, wenn $R/\mathfrak{m}$ genau zwei Ideale enthält (siehe Übung 78); 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 8.

1. Zeigen Sie für $n \in \mathbb{Z}$, dass $\overline{q} \in \mathbb{Z}/n$ genau dann eine Einheit ist, wenn n und q teilerfremd sind.
2. Zeigen Sie allgemeiner: Ist R ein kommutativer Ring und $I \subseteq R$ ein Ideal, so ist $\overline{x} \in R/I$ genau dann eine Einheit, wenn $(x) + I = R$.

Lösung 8.

1. Es ist $\overline{q} \in \mathbb{Z}/n$ genau dann eine Einheit, wenn es $b \in \mathbb{Z}$ mit $\overline{q}\overline{b} = \overline{1}$ gibt. Dies ist äquivalent dazu, dass es $a, b \in \mathbb{Z}$ mit $qb - 1 = an$, also $1 = qb - an$ gibt. Dies ist äquivalent dazu, dass bereits $(n, q) = 1$ gilt. Da $(n, q) = (\text{ggT}(n, q))$ gilt, ist dies wiederum äquivalent dazu, dass $\text{ggT}(n, q) = 1$ gilt, dass also n und q teilerfremd sind.

2. Es sei $\pi\colon R \to R/I, x \mapsto \overline{x}$ die kanonische Projektion. Wir erhalten eine wohldefinierte Bijektion

$$\{\text{Ideale in } R, \text{die } I \text{ enthalten}\} \to \{\text{Ideale in } R/I\}, \quad J \mapsto \pi(J), \quad \pi^{-1}(K) \hookleftarrow K$$

(siehe Übung 6). Inbesondere entspricht das Ideal $(x) + I \subseteq R$ dem Ideal $(\overline{x}) \subseteq R/I$ und das Ideal $R \subseteq R$ den Ideal $R/I \subseteq R/I$. Es ist $\overline{x}$ genau dann eine Einheit in R/I, wenn $(\overline{x}) = R/I$; aufgrund der obigen Bijekton ist dies äquivalent dazu, dass $(x) + I = R$.

Übung 9.

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.
4. Zeigen Sie für jedes weitere Ideal $J \subseteq R$ die Gleichheit $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

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

5. 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.

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

Lösung 9.

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. Aus den Inklusionen $I \cap J \subseteq I, J$ folgen die Inklusionen $\sqrt{I \cap J} \subseteq \sqrt{I}, \sqrt{J}$ und damit die Inklusion $\sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$.

   Ist andererseits $x \in \sqrt{I} \cap \sqrt{J}$, so gibt es $n, m \in \mathbb{N}$ mit $x^n \in I$ und $x^m \in J$. Dann ist $x^{n+m} = x^n x^m \in I \cap J$ (es gilt $x^n x^m \in I$ da $x^n \in I$, und $x^n x^m \in J$ da $x^m \in J$) und deshalb $x \in \sqrt{I \cap J}$.

5. 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

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

6. 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.

7. 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 $x = 0$.

   Alternativ lässt sich die Aussage auch direkt zeigen: Für $x \in R$ und $n \geq 1$ mit $x^n \in \mathfrak{p}$ gilt $x \cdots x \in \mathfrak{p}$, und da $\mathfrak{p}$ prim ist, muss bereits einer der Faktoren in $\mathfrak{p}$ enthalten sein.

Übung 10.
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 10.
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 11. *Die Einheitengruppe des Potenzreihenrings*
Es sei R ein kommutativer Ring. Zeigen Sie, dass $R[\![T]\!]^\times = \{\sum_{i=0}^\infty f_i T^i \in R[\![T]\!] \mid f_0 \in R^\times\}$.

Lösung 11.
Es sei $f = \sum_{i=0}^\infty f_i T^i \in R$.

Ist $f \in R[\![T]\!]^\times$, so gibt es $g = \sum_{i=0}^\infty g_i T^i \in R[\![T]\!]$ mit $fg = 1$. Inbesondere ist dann $f_0 g_0 = 1$ und somit $f_0 \in R^\times$.

Ist andererseits $f_0 \in R^\times$, so seien die Koeffizienten von $g = \sum_{i=0}^\infty g_i T^i \in R[\![T]\!]$ rekursiv durch $g_0 = f_0^{-1}$ und $g_i := -f_0^{-1}\sum_{j=0}^{i-1} f_{i-j} g_j$ definiert. Für $fg = \sum_{i=0}^\infty h_i T^i$ gilt dann $h_0 = f_0 g_0 = 1$, sowie

$$h_i = \sum_{j=0}^{i} f_{i-j} g_j = f_0 g_i + \sum_{j=0}^{i-1} f_{i-j} g_j = -\sum_{j=0}^{i-1} f_{i-j} g_j + \sum_{j=0}^{i-1} f_{i-j} g_j = 0$$

für alle $i \geq 1$, und somit $fg = 1$.

Übung 12. *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 12.

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 $\psi := \phi^{-1}\colon S \to R$. 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 13.

Die Eulersche Phi-Funktion ist definiert als
$$\varphi\colon \mathbb{N}_{>1} \to \mathbb{N}, \quad n \mapsto |\{k \in \{1, \dots, n\} \mid k \text{ und } n \text{ sind teilerfremd}\}|.$$

1. Zeigen Sie, dass $\varphi(n) = |(\mathbb{Z}/n)^\times|$ für alle $n \geq 1$.

2. Folgern Sie, dass $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$ für je zwei teilerfremde $n_1, n_2 \geq 1$.

3. Zeigen Sie, dass $\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$ für alle Primzahlen $p \in \mathbb{N}$ und $r \geq 1$.

4. Berechnen Sie $\varphi(42)$, $\varphi(57)$ und $\varphi(144)$.

Lösung 13.

1. Die Elemente $1, \dots, n$ bilden ein Repräsentantensystem der Restklassen von $\mathbb{Z}/n$, für $k \in \{1, \dots, n\}$ ist $\overline{k} \in \mathbb{Z}/n$ genau dann eine Einheit, wenn k und n teilerfremd sind (siehe Übung 8).

2. Nach dem Chinesischen Restklassensatz gilt $\mathbb{Z}/(n_1 n_2) \cong \mathbb{Z}/n_1 \times \mathbb{Z}/n_2$. Somit gilt

$$\begin{aligned}\varphi(n_1 n_2) &= |(\mathbb{Z}/(n_1 n_2))^\times| = |(\mathbb{Z}/n_1 \times \mathbb{Z}/n_2)^\times| \\ &= |(\mathbb{Z}/n_1)^\times \times (\mathbb{Z}/n_2)^\times| = |(\mathbb{Z}/n_1)^\times||(\mathbb{Z}/n_2)^\times| = \varphi(n_1)\varphi(n_2).\end{aligned}$$

3. Es ist $\{0, \dots, p^r - 1\}$ ein Repräsentantensystem der Restklassen von $\mathbb{Z}/p^r$. Eine Zahl $k \in \{0, \dots, p^r - 1\}$ ist genau dann teilerfremd so p^r, wenn sie kein Vielfaches von p ist. Da jede p-te Zahl aus dieser Menge ein Vielfaches von p ist, gibt es $p^r/p = p^{r-1}$ viele Vielfache von p in diesem Repräsentantensystem. Somit sind $p^r - p^{r-1}$ viele Repräsentanten kein Vielfaches von p, also teilerfremd zu p.

4. Es gelten

$$\begin{aligned}\varphi(42) &= \varphi(2 \cdot 3 \cdot 7) = \varphi(2)\varphi(3)\varphi(7) = (2-1)(3-1)(7-1) = 12, \\ \varphi(57) &= \varphi(3 \cdot 19) = (3-1)(19-1) = 36, \\ \varphi(144) &= \varphi(2^4 \cdot 3^2) = (16-8)(9-3) = 48.\end{aligned}$$

Übung 14. *Der Frobeniushomomorphismus*

Es sei R ein kommutativer Ring mit $p := \operatorname{char} R > 0$ prim.

1. Zeigen Sie, dass die Abbildung $\sigma\colon R \to R$, $x \mapsto x^p$ ein Ringhomomorphismus ist.

2. Zeigen Sie, dass σ ein Automorphismus ist, falls R ein endlicher Körper ist.

Lösung 14.

1. Es gilt $\sigma(1) = 1^p = 1$ und $\sigma(xy) = (xy)^p = x^p y^p = \sigma(x)\sigma(y)$ für alle $x, y \in R$. Es bleibt also nur zu zeigen, dass σ additiv ist. Für alle $x, y \in R$ gilt

$$\sigma(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} \tag{6}$$

   Für alle $k = 1, \dots, p-1$ gilt dabei $p \mid \binom{p}{k}$, denn in dem Ausdruck $\binom{p}{k} = p!/(k!(p-k)!)$ enthält dann zwar der Zähler p als Primfaktor, der Nenner aber nicht, da $k, p-k < p$. Folglich vereinfacht sich (6) zu $\sigma(x+y) = x^p + y^p = \sigma(x) + \sigma(y)$.

2. Es gilt $\ker \sigma = 0$, denn für $x \in R$ mit $x^p = \sigma(x) = 0$ gilt wegen der Nullteilerfreiheit von R bereits, dass $x = 0$. Also ist σ injektiv, und wegen der Endlichkeit von R damit auch schon bijektiv.

Übung 15.
Es sei K ein Körper.

1. Zeigen Sie, dass $(X, Y) \subseteq K[X, Y]$ kein Hauptideal ist.
2. Zeigen Sie, dass das Ideal $(X_i \mid i \in \mathbb{N}) \subseteq K[X_i \mid i \in \mathbb{N}]$ nicht endlich erzeugt ist.
   (*Hinweis*: In jedem Polynom $f \in K[X_i \mid i \in \mathbb{N}]$ kommen nur endlich viele Variablen vor.)

Übung 16. *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 16.
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 17.
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 17.
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 18.
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 18.
1. Für $k \geq 0$ mit $n^k = 0$ gilt $(1 - n)(1 + n + \cdots + n^{k-1}) = 1 - n^k = 1$. 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 19.
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 20.
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 21.
Für jedes $d \in \mathbb{N}$ sei

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

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 22.
Es sei R ein euklidischer Ring. Zeigen Sie, dass R ein Hauptidealring ist.

Lösung 22.
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 23.
Es sei R ein Hauptidealring. Zeigen Sie, dass jedes Primideal in R bereits ein maximales Ideal ist.

Lösung 23.
Es sei $\mathfrak{m} \subseteq R$ ein Primideal und $p \in R$ mit $\mathfrak{m} = (p)$; inbesondere ist p prim. Es sei $\mathfrak{a} \subseteq R$ ein Ideal mit $\mathfrak{m} \subseteq \mathfrak{a}$ und $a \in R$ mit $\mathfrak{a} = (a)$. Dass $(p) \subseteq (a)$ gilt, ist äquivalent dazu, dass $a \mid p$ gilt; es gibt also $b \in R$ mit $p = ab$. Da p prim ist, gilt bereits $p \mid a$ oder $p \mid b$.

Gilt $p \mid b$, so gibt es $c \in R$ mit $b = pc$. Dann gilt $p = ab = abp$ und somit $1 = ab$, da R ein Integritätsbereich ist. In diesem Fall ist also a eine Einheit und somit $\mathfrak{a} = (a) = R$ kein echtes Ideal.

Gilt andererseits $p \mid a$, so ist $\mathfrak{a} = (a) \subseteq (p) = \mathfrak{m}$, und somit bereits $\mathfrak{m} = \mathfrak{a}$.

Ingesamt zeigt dies, dass es kein echtes Ideal $\mathfrak{b} \subsetneq R$ gibt, so dass $\mathfrak{m} \subsetneq \mathfrak{b}$. Da $\mathfrak{m}$ als Primideal inbesondere ein echtes Ideal ist, folgt daraus, dass $\mathfrak{m}$ ein maximales Ideal ist.

Übung 24.
Es sei K ein kommutativer Ring, so dass $K[X]$ ein Hauptidealring ist. Zeigen Sie, dass K bereits ein Körper ist.

Lösung 24.
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
$$(a, X) = (f). \tag{7}$$
Wegen Gleichung (7) 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 $f = f_0 = a_0 p_0 = ap_0$. 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 $h(X) = b_1 X + b_0$ 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 25.
Es sei R ein kommutativer Ring, $(a_i)_{i \in I}$ eine Familie von Elementen $a_i \in R$ und $a \in R$.

1. Zeigen Sie, dass a ein größter gemeinsamer Teiler der a_i ist, falls $(a_i \mid i \in I) = (a)$.

2. Entscheiden Sie, ob auch die Umkehrung der obigen Aussage gilt.

Übung 26.
1. Es ist a ein gemeinsamer Teiler der a_i, denn es gilt

$$(a_i \mid i \in I) \subseteq (a) \iff \forall i \in I : a_i \in (a) \iff \forall i \in I : a \mid a_i.$$

   Da außerdem $a \in (a) \subseteq (a_i \mid i \in I)$ gilt, ergibt sich $a = \sum_{i \in I} r_i a_i$ für passende $r_i \in R$ mit $r_i = 0$ für fast alle $i \in I$. Für jeden gemeinsamen Teiler $b \in R$ der a_i gilt deshalb auch $b \mid a$. Somit ist a bereits ein größter gemeinsamer Teiler der a_i.

2. Die Umkehrung gilt im Allgemeinen nicht: Ist etwa K ein Körper, so ist 1 ein größter gemeinsamer Teiler von $X, Y \in K[X, Y]$, aber $(X, Y) \subsetneq (1)$.

Übung 27. *Euklid*
Es sei K ein Körper. Zeigen Sie, dass es in $K[X]$ unendlich viele normierte, irreduzible Polynome gibt.

Lösung 27.
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

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

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 28.
Es sei R ein Ring und $I \subseteq R$ ein echtes Ideal. Zeigen Sie mithilfe des Lemmas von Zorn, dass es ein maximales Ideal $\mathfrak{m} \subsetneq R$ gibt, so dass $I \subseteq \mathfrak{m}$.

Lösung 28.
Es sei

$$\mathcal{I} \coloneqq \{J \subsetneq R \mid J \text{ ist ein echtes Ideal mit } I \subseteq J\}.$$

Die Menge $\mathcal{I}$ ist nicht leer, da sie I enthält. Bezüglich der üblichen Teilmengeninklusion $\subseteq$ ist $\mathcal{I}$ partiell geordnet.

Ist $\mathcal{K} \subseteq \mathcal{I}$ eine nicht-leere Kette, so ist auch $K \coloneqq \bigcup \mathcal{K} = \bigcup_{J \in \mathcal{K}} J$ wieder ein Ideal in R, und es gilt $I \subseteq K$. Da alle $J \in \mathcal{K}$ echte Ideale sind, gilt $1 \notin J$ für alle $J \in \mathcal{K}$; somit gilt auch $1 \notin K$, weshalb K ein echtes Ideal in R ist. Ingesamt ist also $K \in \mathcal{I}$, und da $J \subseteq K$ für alle $J \in \mathcal{K}$ gilt, ist K eine obere Schranke für $\mathcal{K}$ in $\mathcal{I}$.

Nach dem Lemma von Zorn besitzt nun $\mathcal{I}$ ein maximales Element $\mathfrak{m} \in \mathcal{I}$; inbesondere ist $\mathfrak{m}$ ein echtes Ideal in R mit $I \subseteq \mathfrak{m}$. Wäre $\mathfrak{m}$ kein maximales Ideal in R, so gebe es ein echtes Ideal $\mathfrak{m}' \subsetneq R$ mit $\mathfrak{m} \subsetneq \mathfrak{m}'$. Dann wäre aber $I \subseteq \mathfrak{m} \subsetneq \mathfrak{m}'$ und somit $\mathfrak{m}' \in \mathcal{I}$. Da $\mathfrak{m} \subsetneq \mathfrak{m}'$ stünde dies im Widerspruch zur Maximalität von $\mathfrak{m}$ in $\mathcal{I}$. Also muss $\mathfrak{m}$ bereits ein maximales Ideal in R sein.

Übung 29.
Es sei R ein kommutativer Ring und $\mathfrak{a} \subseteq R$ ein Ideal.

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

$$\mathfrak{a}[X] \coloneqq \left\{ \sum_i f_i X^i \in R[X] \;\middle|\; f_i \in \mathfrak{a} \text{ für alle } i \right\}$$

   ein Ideal in $R[X]$ ist.

2. Zeigen Sie, dass die Abbildung

$$R[X]/\mathfrak{a}[X] \to (R/\mathfrak{a})[X], \quad \overline{\sum_i a_i X^i} \mapsto \sum_i \overline{a_i} X^i$$

   ein wohldefinierter Isomorphismus ist.

3. Zeigen Sie, dass für jedes Primideal $\mathfrak{p} \subseteq R$ auch $\mathfrak{p}[X] \subseteq R[X]$ ein Primideal ist.

4. Zeigen oder widerlegen Sie, dass für jedes maximale Ideal $\mathfrak{m} \subseteq R$ auch $\mathfrak{m}[X] \subseteq R[X]$ ein maximales Ideal ist.

Das Ideal $\mathfrak{a}[X]$ lässt sich auch noch anders durch $\mathfrak{a}$ beschreiben.

5. Zeigen Sie, dass $\mathfrak{a}[X]$ das von $\mathfrak{a}$ in $R[X]$ erzeugte Ideal ist, d.h. dass $(\mathfrak{a})_{R[X]} = \mathfrak{a}[X]$.

Damit erhalten wir für jedes Ideal $\mathfrak{a} \subseteq R$ einen Ringisomorphismus $R[X]/(\mathfrak{a}) \to (R/\mathfrak{a})[X]$, $\overline{\sum_i a_i X^i} \mapsto \sum_i \overline{a_i} X^i$.

6. Veinfachen Sie für die folgenden Ringe R und Ideale $I \subseteq R$ jeweils den Quotienten R/I. Entscheiden Sie jeweils, ob das Ideal prim oder maximal ist.

$$(7) \subseteq \mathbb{Z}[X], \quad (3, X^2+1) \subseteq \mathbb{Z}[X], \quad (5, X^2+X+3) \subseteq \mathbb{Z}[X], \quad (X^2+1) \subseteq \mathbb{Q}[X,Y].$$

Lösung 29.

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

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

   Nach dem vorherigen Aussagenteil gilt $\ker\psi = \mathfrak{a}[X]$, was die Aussage zeigt.

3. Der Quotient $R/\mathfrak{p}$ ist ein Integritätsbereich, da $\mathfrak{p}$ ein Primideal in R ist. Damit ist auch $(R/\mathfrak{p})[X] \cong R[X]/\mathfrak{p}[X]$ ein Integritätsbereich ist, und deshalb $\mathfrak{p}[X]$.

4. 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 30).

5. Es gilt $\mathfrak{a} \subseteq \mathfrak{a}[X]$ und somit $(\mathfrak{a})_{R[X]} \subseteq \mathfrak{a}[X]$. Andererseits ist $aX^i \in (\mathfrak{a})_{R[X]}$ für jedes $a \in \mathfrak{a}$ und $i \geq 0$ und somit $\sum_i a_i X^i \in\in (\mathfrak{a})_{R[X]}$ für jedes $\sum_i a_i X^i \in \mathfrak{a}[X]$.

6. a) Es gilt $\mathbb{Z}[X]/(7) \cong (\mathbb{Z}/7)[X] = \mathbb{F}_7[X]$. Das Ideal ist also prim, aber nicht maximal.

   b) Mithilfe des dritten Isomorphiesatzes erhält man, dass

$$\begin{aligned}\mathbb{Z}[X]/(3, X^2+1) &\cong (\mathbb{Z}[X]/(3))/((3, X^2+1)/(3)) = (\mathbb{Z}[X]/(3))/(\overline{X^2+1}) \\ &\cong (\mathbb{Z}/3)[X]/(X^2+1) = \mathbb{F}_3[X]/(X^2+1).\end{aligned}$$

   Das Polynom $X^2 + 1 \in \mathbb{F}_3[X]$ ist quadratisch und hat keine Nullstellen, ist also irreduzibel. Der obige Quotient ist also eine Körpererweiterung von $\mathbb{F}_3$ von Grad 2, also $\mathbb{F}_3[X]/(X^2+1) \cong \mathbb{F}_9$. Inbesondere ist das Ideal maximal.

   c) Mithilfe des dritten Isomorphiesatzes erhält man, dass

$$\begin{aligned}&\mathbb{Z}[X]/(5, X^2+6X-2) \cong (\mathbb{Z}[X]/(5))/((5, X^2+6X-2)/(5)) \\ \cong\ &(\mathbb{Z}[X]/(5))/(\overline{X^2+6X-2}) \cong (\mathbb{Z}/5)[X]/(X^2+6X-2) \\ \cong\ &\mathbb{F}_5[X]/(X^2-4X+3) = \mathbb{F}_5[X]/((X-1)(X-3)).\end{aligned}$$

Mithilfe des chinesischen Restklassensatzes erhält man weiter, dass

$$\mathbb{F}_5[X]/((X-1)(X-3)) \cong \mathbb{F}_5[X]/(X-1) \times \mathbb{F}_5[X]/(X-3) \cong \mathbb{F}_5 \times \mathbb{F}_5.$$

Da $\mathbb{F}_5 \times \mathbb{F}_5$ kein Integritätsbereich ist, ist das Ideal nicht prim.

d) Es gilt

$$\mathbb{Q}[X,Y]/(X^2+1) \cong \mathbb{Q}[X][Y]/(X^2+1) \cong (\mathbb{Q}[X]/(X^2+1))[Y] \cong \mathbb{Q}(i)[Y].$$

Inbesondere ist das Ideal prim, aber nicht maximal.

Übung 30.
Zeigen Sie, dass es keinen Ring R gibt, so dass $R[X]$ ein Körper ist.

Lösung 30.
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 31.
Es seien $R_1, \dots, R_n$ kommutative Ringe für jedes $i = 1, \dots, n$ sei $\mathfrak{a}_i \subseteq R_i$ ein Ideal.

1. Zeigen Sie, dass $\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n$ ein Ideal in $R_1 \times \cdots \times R_n$ ist.
2. Zeigen Sie, dass $(R_1 \times \cdots R_n)/(\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n) \cong (R_1/\mathfrak{a}_1) \times \cdots \times (R_n/\mathfrak{a}_n)$ gilt.
3. Folgern Sie, dass $\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n$ genau dann prim ist, wenn es ein $1 \leq j \leq n$ gibt, so dass $\mathfrak{a}_j \subseteq R_j$ prim ist, und $\mathfrak{a}_i = R_i$ für alle $i \neq j$ gilt.
4. Entscheiden Sie, ob die obige Aussage auch für maximale Ideale gilt.

Lösung 31.
1. Für jedes $i = 1, \dots, n$ sei $\pi_i \colon R_i \to R_i/\mathfrak{a}_i$, $x \mapsto \overline{x}$ die kanonische Projektion. Es ist

$$R_1 \times \cdots \times R_n \xrightarrow{\pi := \pi_1 \times \cdots \times \pi_n} (R_1/\mathfrak{a}_1) \times \cdots \times (R_n/\mathfrak{a}_n)$$

ein Ringhomomorphismus mit $\ker \pi = (\ker \pi_1) \times \cdots \times (\ker \pi_n) = \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n$. Inbesondere ist deshalb $\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n$ ein Ideal in $R_1 \times \cdots \times R_n$.

2. Da die π_i surjektiv sind, ist es auch π. Da $\ker \pi = \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n$ gilt, induziert π also einen Isomorphismus

$$\begin{aligned} \overline{\pi} \colon (R_1 \times \cdots \times R_n)/(\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n) &\to (R_1/\mathfrak{a}_1) \times \cdots \times (R_n/\mathfrak{a}_n), \\ \overline{(x_1, \dots, x_n)} &\mapsto (\overline{x_1}, \dots, \overline{x_n}). \end{aligned}$$

3. Ist $\mathfrak{a}_i \neq R_i$ und $\mathfrak{a}_j \neq R_j$ für $i \neq j$, so sind in dem Produkt $(R_1/\mathfrak{a}_1) \times \cdots \times (R_n/\mathfrak{a}_n)$ mindestens zwei Faktoren nicht trivial, und der Ring somit nicht nullteilerfrei. Es genügt daher, sich auf den Fall einzuschränken, dass $\mathfrak{a}_i = R_i$ für alle $i = 1, \ldots, n$ bis auf ein $1 \leq j \leq n$. Dann gilt

$$\begin{aligned}(R_1 \times \cdots R_n)/(\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n) &\cong (R_1/\mathfrak{a}_1) \times \cdots \times (R_n/\mathfrak{a}_n) \\ &\cong 0 \times \cdots \times 0 \times (R_j/\mathfrak{a}_j) \times 0 \times \cdots \times 0 \cong R_j/\mathfrak{a}_j,\end{aligned}$$

und somit

$$\begin{aligned}&\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n \text{ ist prim} \\ \iff &(R_1 \times \cdots R_n)/(\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n) \text{ ist ein Integritätsbereich} \\ \iff &R_j/\mathfrak{a}_j \text{ ist ein Integritätsbereich} \iff \mathfrak{a}_j \text{ ist prim.}\end{aligned}$$

4. Die Aussage gilt auch für maximale Ideale. Man muss nur in der obigen Argumentation *prim* durch *maximal* und *Integritätsbereich* durch *Körper* ersetzen.

Übung 32.
Es seien $R_1, \ldots, R_n$ kommutative Ringe Zeigen Sie, dass jedes Ideal $\mathfrak{a} \subseteq R_1 \times \cdots \times R_n$ von der Form $\mathfrak{a} = \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n$ für eindeutige Ideale $\mathfrak{a}_i \subseteq R_i$ ist.

Lösung 32.
Die Eindeutigkeit ist klar, und es gilt nur die Existenz zu zeigen: Für jedes $i = 1, \ldots, n$ sei $\pi_i \colon R_1 \times \cdots \times R_n \to R_i, (x_1, \ldots, x_n) \mapsto x_i$ die kanonische Projektion. Für jedes $i = 1, \ldots, n$ sei außerdem $e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in R_1 \times \cdots \times R_n$ das Element, dessen i-ter Eintrag 1 ist, und dessen Einträge sonst alle 0 sind. Für alle $i = 1, \ldots, n$ sei $\mathfrak{a}_i \coloneqq \pi_i(\mathfrak{a})$.

Es gilt $\mathfrak{a} \subseteq \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n$, denn für jedes $(x_1, \ldots, x_n) \in \mathfrak{a}$ gilt $x_i = \pi(x) \in \mathfrak{a}_i$ für alle $i = 1, \ldots, n$ und somit $x \in \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n$.

Ist andererseits $x = (x_1, \ldots, x_n) \in \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n$, so ist $x_i \in \mathfrak{a}_i$ für alle $i = 1, \ldots, n$. Für alle $i = 1, \ldots, n$ gibt es deshalb ein $y^{(i)} = (y_1^{(i)}, \ldots, y_n^{(i)}) \in \mathfrak{a}$ mit $\pi_i(y^{(i)}) = x_i$, also $y_i^{(i)} = x_i$. Es folgt, dass

$$\begin{aligned}x = (x_1, \ldots, x_n) &= \sum_{i=1}^{n} \underbrace{(0, \ldots, 0, x_i, 0, \ldots, 0)}_{x_i \text{ an } i\text{-ter Stelle}} \\ &= \sum_{i=1}^{n} e_i \left(y_1^{(i)}, \ldots, y_{i-1}^{(i)}, x_i, y_{i+1}^{(i)}, \ldots, y_n^{(i)}\right) = \sum_{i=1}^{n} e_i y^{(i)} \in \mathfrak{a}.\end{aligned}$$

Bemerkung. Übung 31 und Übung 32 ergeben zusammen eine Klassifikation der Primideale, bzw. maximalen Ideale in $R_1 \times \cdots \times R_n$: Es handelt sich (in gewisser Weise) um die disjunkte Vereinigung der Primideale, bzw. maximalen Ideale der R_i.

Übung 33.
Zeigen Sie, dass $\mathbb{Z}[i] \cong \mathbb{Z}[X]/(X^2+1)$.

Übung 34.
Es sei R ein Integritätsbereich. Zeigen Sie, dass $Q(R[X]) \cong Q(R)(X)$.

Übung 35.
Es sei $f\colon R \to R'$ ein Ringhomomorphismus zwischen kommutativen Ringen R und R'. Es sei $S \subseteq R$ eine multiplikative Menge.

1. Zeigen Sie, dass $S' \coloneqq f(S)$ eine multiplikative Menge in R' ist.

2. Zeigen Sie, dass es einen eindeutigen Ringhomomorphismus $\hat{f}\colon R \to R'$ gibt, so dass das folgende Diagramm kommutiert:

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

   Hierbei sind die unbenannten vertikalen Pfeile jeweils die kanonischen Ringhomomorphismen.

Lösung 35.
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 $\hat{f}\colon R_S \to R'_{S'}$ mit $\hat{f}i = i'f$, d.h. so dass das folgende Diagram kommutiert:

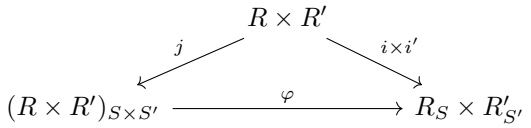
$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i'} \\ R_S & \xrightarrow{\hat{f}} & R'_{S'} \end{array}$$

Übung 36.
Es seien R und R' zwei kommutative Ringe, und $S \subseteq R$ und $S' \subseteq R'$ multiplikative Mengen. Es seien $i\colon R \to R_S$ und $i'\colon R' \to R'_{S'}$ die kanonischen Ringhomomorphismen.

1. Zeigen Sie, dass $S \times S' \subseteq R \times R'$ eine multiplikative Menge ist.

Es sei $j\colon R \times R' \to (R \times R')_{S \times S'}$ der kanonische Ringhomomorphismus.

2. Zeigen Sie, dass es eine eindeutigen Ringhomomorphismus $\varphi\colon (R\times R')_{S\times S'} \to R_S \times R'_{S'}$ gibt, so dass das folgende Diagram kommutiert:



3. Zeigen Sie, dass φ ein Isomorphismus ist.

Übung 37.
Es sei R ein kommutativer Ring und $f \in R$. Zeigen Sie, dass $R_f \cong R[X]/(fX-1)$.

Lösung 37.
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 38.
Bestimmen Sie die Einheitengruppe $\mathbb{Z}[i]^\times$.

Lösung 38.
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

$$1 = |1|^2 = |zz^{-1}|^2 = |z|^2|z^{-1}|. \tag{8}$$

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 (8) 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 39.
Formulieren und beweisen Sie den Hilbertschen Basissatz.

Übung 40. *Ein Lemma von Gauß*
Es sei R ein faktorieller Ring und $f, g \in R[T]$ seien zwei primitive Polynome. Zeigen Sie, dass auch fg primitiv ist.

Übung 41.
Wir nehmen an, dass fg nicht primitiv ist. Dann gibt es ein Primelement $p \in R$, dass alle Koeffizienten von fg teilt. Für den von der kanonischen Projektion $R \to R/(p)$, $r \mapsto \overline{r}$ induzierten Ringhomomorphismus $\varphi\colon R[T] \to (R/(p))[T]$ gilt dann $0 = \varphi(fg) = \varphi(f)\varphi(g)$. Der Quotient $R/(p)$ ist ein Integritätsbereich, da p prim ist, und $(R/(p))[T]$ somit ebenfalls. Also muss bereits $\varphi(f) = 0$ oder $\varphi(g) = 0$. Dann sind aber alle Koeffizienten von f durch p teilbar, oder alle Koeffizienten von g durch p teilbar, was der Primitivität von f und g widerspricht.

Übung 42.
Es sei K ein Körper und $R \coloneqq K[t^2, t^3] \subseteq K[t]$.

1. Zeigen Sie, dass R noethersch ist.
2. Folgern Sie, dass in R eine Zerlegung in irreduzible Elemente existiert.
3. Zeigen Sie, dass R nicht faktoriell ist. (*Hinweis*: Zeigen Sie zunächst, dass t^2 und t^3 irreduzibel sind.)

Lösung 42.

1. Nach dem Hilbertschen Nullstellensatz ist $K[X,Y]$ noethersch. Der Einsetzhomomorphismus $\varphi\colon K[X,Y] \to K[t^2,t^3]$ mit $\varphi(X) = t^2$ und $\varphi(Y) = t^3$ ist surjektiv, und somit $R = K[t^2,t^3] \cong K[X,Y]/\ker\varphi$ als Quotient eines noetherschen Rings ebenfalls noethersch.

2. Als Unterring von $K[t]$ ist R ein Integritätsbereich. Aus der Vorlesung ist bekannt, dass in noetherschen Integritätsbereichen eine Zerlegung in irreduzible Elemente existiert.

3. Wir bemerken zunächst, dass $R = \{\sum_i f_i T^i \in K[t] \mid f_1 = 0\}$. Es enthält also R keine Polynome vom Grad 1. Jede nicht-triviale Zerlegung von t^2 oder t^3 in $K[t]$ enthält aber einen Faktor vom Grad 1; folglich sind beide Elemente irreduzibel in R. Wir erhalten nun für $t^6 \in R$ mit $t^6 = t^2 \cdot t^2 \cdot t^2 = t^3 \cdot t^3$ zwei Zerlegungen in irreduzible Elemente, die nicht äquivalent im Sinne eines faktoriellen Rings sind (insbesondere kommen in beiden Zerlegungen unterschiedlich viele Faktoren vor). Folgich ist R nicht faktoriell.

Übung 43.

Es sei K ein Körper. Zeigen Sie, dass der Ring $K[\![X]\!]$ ein eindeutiges maximales Ideal besitzt.

Lösung 43.

Wir geben zwei mögliche Beweise an:

1. Der Ring $K[\![X]\!]$ ein ein euklidisch mit der üblichen Gradabbildung Deg und somit ein Hauptidealring. Also ist jedes Ideal in $K[\![X]\!]$ von der Form (f) für ein Element $f \in K[\![X]\!]$. Ist $f \in K[\![X]\!]$ mit $f \neq 0$, so ist $f = \sum_{i=n}^{\infty} f_i X^i$ mit $f_n \neq 0$ für ein $n \geq 0$. Dann ist

$$f = \sum_{i=n}^{\infty} f_i X^i = X^n \cdot \sum_{j=0}^{\infty} f_{n+j} X^j = X^n \cdot g.$$

   für das Element $g \coloneqq \sum_{j=0}^{\infty} f_{n+j} X^j$. Es gilt $g_0 \neq 0$, also $g_0 \in K^\times$, und somit $g \in K[\![X]\!]^\times$. Also sind f und X^n assoziiert, und somit $(f) = (X^n)$.

   Damit ist gezeigt, dass 0 und die Ideale (X^n) für $n \geq 0$ die einzigen Ideale in $K[\![X]\!]$ sind. Falls $(X^n) = (X^m)$ mit $n \leq m$, so sind X^n und X^m assoziiert zueinander, und es gibt $g \in K[\![X]\!]^\times$ mit $X^n = gX^m$. Dann gilt $g_0 \neq 0$ und somit $\operatorname{Deg} gX^m = m$, weshalb $n = \operatorname{Deg} X^n = \operatorname{Deg} gX^m = m$. Die Ideale in $K[\![X]\!]$ bilden also eine echte absteigende Kette

$$(1) = (X^0) \supsetneq (X) \supsetneq (X^2) \supsetneq (X^3) \supsetneq (X^4) \supsetneq \cdots \supsetneq 0.$$

   Inbesondere ist (X) das eindeutige maximale Ideal in $R[\![X]\!]$.

2. Es sei $\mathfrak{m} \coloneqq \{f \in K[\![X]\!] \mid f_0 = 0\}$. Die Abbildung $\varphi\colon K[\![X]\!] \to K$, $f \mapsto f_0$ ist ein Ringhomomorphismus mit $\ker\varphi = \mathfrak{m}$, weshalb $\mathfrak{m}$ ein Ideal in $K[\![X]\!]$ ist. Da

$$K = \operatorname{im}\varphi \cong K[\![X]\!]/\ker\varphi = K[\![X]\!]/\mathfrak{m}$$

   ein Körper ist, ist $\mathfrak{m}$ bereits ein maximales Ideal.

Gebe es ein maximales Ideal $\mathfrak{m}' \subseteq K[\![X]\!]$ mit $\mathfrak{m}' \neq \mathfrak{m}$, so würde wegen der Maximalität von $\mathfrak{m}'$ inbesondere $\mathfrak{m}' \nsubseteq \mathfrak{m}$ gelten. Dann gebe es $f \in \mathfrak{m}'$ mit $f \notin \mathfrak{m}$, also $f_0 \neq 0$ und somit $f \in K^\times$. Dann würde aber $f \in K[\![X]\!]^\times$ gelten, und somit $(1) = (f) \subseteq \mathfrak{m}'$, was im Widerspruch dazu stünde, dass $\mathfrak{m}'$ ein echtes Ideal in $K[\![X]\!]$ ist.

2 Modultheorie

Übung 44. *Multiple Choice*
Es sei R ein kommutativer Ring. Entscheiden Sie, welche der folgenden Aussagen wahr oder falsch sind.

1. Ist M ein freier R-Modul und $S \subseteq R$ ein Unterring, so ist M auch als S-Modul frei.
2. Ist M ein freier R-Modul endlichen Rangs, so ist auch jeder Untermodul $N \subseteq M$ frei.
3. Ist jeder R-Modul frei, so ist R ein Körper.
4. Ist M ein R-Modul und $N \subseteq M$ ein Untermodul, so gibt es einen Untermodul $P \subseteq M$ mit $M = N \oplus P$.
5. Sind M und N zwei freie R-Moduln endlichen Rangs, so ist auch $\mathrm{Hom}_R(M, N)$ ein freier R-Modul.
6. Ist M ein endlich erzeugter R-Modul, so ist auch jeder Untermodul $N \subseteq M$ endlich erzeugt.
7. Ist M ein R-Modul, so dass jedes Element $m \in M$ bereits in einem endlichen Untermodul von M enthalten ist, so ist M endlich erzeugt.
8. Ist M ein endlich erzeugter R-Modul und $E \subseteq M$ ein minimales Erzeugendensystem, so ist E endlich.
9. Ist M ein endlich erzeugter R-Modul und $E_1, E_2 \subseteq M$ zwei minimale Erzeugendensysteme, so sind E_1 und E_2 gleichmächtig.
10. Ist $0 \to N \to M \to P \to 0$ eine kurze exakte Sequenz von R-Moduln mit $M = N \oplus P$, so spaltet die Sequenz.
11. Ist M ein R-Modul mit $M \cong M \oplus M$, so gilt $M = 0$.
12. Es gibt eine $K[T]$-Modulstruktur auf dem Vektorraum $K[T]$, so dass $X.f = f$ für alle $f \in K[X]$.
13. Es sei $R = K[T]$ und M der eindeutige R-Modul, der dem K-Vektorraum $K[T]$ zusammen mit dem Endomorphismus $D\colon K[T] \to K[T]$, $f \mapsto f'$ entspricht. Dann ist M ein endlich erzeugter R-Modul.

Lösung 44.
1. Die Aussage ist falsch: Betrachtet man etwa $R = \mathbb{Q}$ und $S = \mathbb{Z}$, so ist $M = \mathbb{Q}$ als R-Modul endlich frei vom Rang 1, aber als $\mathbb{Z}$-Modul nicht frei.
2. Die Aussage ist falsch:
3. Die Aussage ist falsch:

4. Die Aussage ist falsch: Für $R = 0$ ist 0 (bis auf Isomorphie) der einzige R-Modul und somit jeder R-Modul frei, aber 0 ist kein Körper.

5. Die Aussage ist wahr: Ist M vom Rang r und N vom Rang s, so gilt

$$\mathrm{Hom}_R(M, N) \cong \mathrm{Mat}(s \times r, R) \cong R^{rs}$$

als R-Moduln.

6. Die Aussage ist falsch: Es sei R ein Ring, so dass es ein Ideal $I \subseteq R$ gibt, das nicht endlich erzeugt ist (man siehe etwa Übung 15). Dann ist R ein endlich erzeugter R-Modul (denn R ist als R-Modul frei vom Rang 1), aber I ist ein Untermodul von R, der nicht endlich erzeugt ist.

7. Die Aussage ist falsch: Ist etwa K ein endlicher Körper und V ein unendlichdimensionaler K-Vektorraum, so ist jedes Element $v \in V$ in dem endlichen Untervektorraum $\langle v \rangle_K$ enthalten, aber V ist als K-Vektorraum nicht endlich erzeugt.

8. Die Aussage ist wahr:

9. Die Aussage ist falsch:

10. Die Aussage ist falsch:

11. Die Aussage ist falsch: Man betrachten etwa den Modul $M = \bigoplus_{n \in \mathbb{N}} R$.

12. Die Aussage ist falsch.

13. Die Aussage ist wahr.

Übung 45.
Zeigen Sie, dass es auf jeder abelschen Gruppe genau eine $\mathbb{Z}$-Modulstruktur gibt.

Lösung 45.
Es sei A eine abelsche Gruppe. Aus der Vorlesung ist die Bijektion

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

bekannt. Dabei ist

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

ein Ring unter punktweiser Adddition und Komposition. Da es genau einen Ringhomomorphismus $\mathbb{Z} \to \mathrm{End}(A)$ gibt (siehe Übung 3) folgt die Aussage.

Übung 46.
Es sei R ein kommutativer Ring und M ein R-Modul. Zeigen Sie, dass $\mathrm{Hom}_R(R, M) \cong M$ als R-Moduln.

Lösung 46.
Wir zeigen, dass die Abbildung $\varphi\colon \mathrm{Hom}_R(R, M) \to M$, $f \mapsto f(1)$ ein Isomorphismus von R-Moduln ist: Dass φ ein Homomorphismus von R-Moduln ist, ergibt sich direkt daraus, dass die R-Modulstruktur auf $\mathrm{Hom}_R(R, M)$ punktweise definiert ist. Die Injektivität von φ ergibt sich daraus, dass $R = \langle 1 \rangle_R$, und somit jeder R-Modulhomomorphismus $f\colon R \to M$ durch die Einschränkung $f|_{\{1\}}$ bereits eindeutig bestimmt ist. Für jedes $m \in M$ ergibt sich ein Homomorphismus von R-Moduln $f_m\colon R \to M$, $r \mapsto rm$; für diesen gilt $\varphi(f_m) = f_m(1) = m$, was die Surjektivität von φ zeigt.

Übung 47.
Es sei R ein Ring und $e\colon M \to M$ ein idempotenter Endomorphismus eines R-Moduls M, d.h. es gilt $e^2 = e$. Zeigen Sie, das $M = \operatorname{im} e \oplus \ker e$ und dass $e(m + m') = m$ für alle $m \in \operatorname{im} e$ und $m' \in \ker e$.

Lösung 47.
Es gilt $M = \operatorname{im} e + \ker e$, denn jedes $m \in M$ lässt sich als $m = e(m) + m - e(m)$ schreiben, wobei $e(m) \in \operatorname{im} e$ und $m - e(m) \in \ker(e)$ (denn $e(m - e(m)) = e(m) - e^2(m) = 0$). Für jedes $m \in M$ gilt $e(m) = m$, denn es gibt ein $\tilde{m} \in M$ mit $m = e(\tilde{m})$, und somit gilt $e(m) = e(e(\tilde{m})) = e^2(\tilde{m}) = e(\tilde{m}) = m$. Für $m \in \operatorname{im} e \cap \ker e$ folgt, dass $m = e(m) = 0$; deshalb gilt $\operatorname{im} e \cap \ker e = 0$.

Übung 48.
Es sei R ein kommutativer Ring und M ein R-Modul. Es sei $I \subseteq R$ ein Ideal und $S \subseteq R$ eine multiplikative Menge.

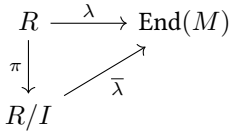
1. Zeigen Sie, dass sich die R-Modulstruktur auf M genau dann zu einer R/I-Modulstruktur fortsetzen lässt, wenn $IM = 0$ (d.h. wenn $am = 0$ für alle $a \in I$ und $m \in M$). Entscheiden Sie, ob diese Fortsetzung eindeutig ist.

2. 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. Entscheiden Sie, ob diese Fortsetzung eindeutig ist.

Lösung 48.
Es sei $\mathrm{End}(M) \coloneqq \{f\colon M \to M \mid f \text{ ist additiv}\}$. Die R-Modulstruktur auf M entspricht dem Ringhomomorphismus $\lambda\colon R \to \mathrm{End}(M)$, $r \mapsto \lambda_r$ mit $\lambda_r(m) = r \cdot m$ für alle $r \in R$, $m \in M$.

1. Es sei $\pi\colon R \to R/I$, $r \mapsto \overline{r}$ die kanonische Projektion. Eine R/I-Modulstruktur auf M entspricht genau einem Ringhomomorphismus $\overline{\lambda}\colon R/I \to \mathrm{End}(M)$. Dass es sich um eine

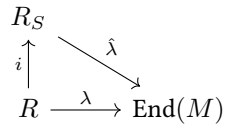
Fortsetzung der R-Modulstruktur handelt, ist dabei äquivalent dazu, dass $\overline{\lambda}$ eine Forsetzung von λ ist, d.h. dass das folgende Diagramm kommutiert:



Nach der universellen Eigenschaft des Quotienten R/I ist eine solche Fortsetzung $\overline{\lambda}$ eindeutig, und sie existiert genau dann, wenn $I \subseteq \ker \lambda$. Es bleibt zu zeigen, dass genau dann $I \subseteq \ker \lambda$, wenn $IM = 0$. Dies ergibt sich daraus, dass für alle $r \in R$

$$r \in \ker \lambda \iff \lambda_r = 0 \iff \forall m \in M : \lambda_r(m) = 0 \iff \forall m \in M : r \cdot m = 0.$$

2. Es sei $i\colon R \to R_S$, $r \mapsto r/1$ der kanonische Ringhomomorphismus. Eine R_S-Modulstruktur auf M entspricht einen Ringhomomorphismus $\hat{\lambda}\colon R_S \to \mathrm{End}(M)$. Dass es sich dabei um eine Forsetzung der R-Modulstruktur handelt, ist äquivalent dazu, dass $\hat{\lambda}$ eine Fortsetzung von λ ist, d.h. dass das folgende Diagramm kommutiert:



Nach der universellen Eigenschaft der Lokalisierung R_S ist eine solche Fortsetzung $\hat{\lambda}$ eindeutig, und sie existiert genau dann, wenn $\lambda(s)$ für jedes $s \in S$ eine Einheit in $\mathrm{End}(M)$ ist. Da ein Element $f \in \mathrm{End}(M)$ genau dann eine Einheit ist, wenn f bijektiv ist, ist die obige Bedingung äquivalent dazu, dass λ_s für alle $s \in S$ bijektiv ist.

Übung 49.
Es sei M ein endlich erzeugter R-Modul. Zeigen Sie, dass jedes Erzeugendensystem $S \subseteq M$ ein endliches Erzeugendensystem enthält.

Lösung 49.
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 50.

Es sei R ein Ring und $0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0$ ein kurze exakte Sequenz von R-Moduln und $M' \subseteq M$ ein Untermodul. Zeigen sie, dass auch

$$0 \to f^{-1}(M') \xrightarrow{f'} M' \xrightarrow{g'} g(M') \to 0$$

eine kurze exakte Sequenz ist, wobei $f' \colon f^{-1}(M') \to M', m \mapsto f(m)$ und $g' \colon M' \to g(M')$, $m \mapsto g(m)$ die entsprechenden Einschränkungen von f und g bezeichnen.

Lösung 50.

Es ist klar, dass f' und g' wohldefinierte Homomorphismen sind. Die Injektivität von f' folgt aus der von f, und die Surjektivität von g' aus $\operatorname{im} g' = g'(M') = g(M')$. Da $g \circ f = 0$ gilt, gilt auch $g' \circ f' = 0$, also $\operatorname{im} f' \subseteq \ker g'$. Ist andererseits $m \in \ker g'$, so gilt $m \in \ker g = \operatorname{im} f$, weshalb es $n \in N$ mit $f(n) = m$ gibt. Dabei gilt bereits $n \in f^{-1}(M')$, da ja $f(n) = m \in M'$, und somit $m = f(n) = f'(n) \in \operatorname{im} f'$. Das zeigt, dass auch $\ker g' \subseteq \operatorname{im} f'$.

Übung 51.

Es sei R ein Hauptidealring und F ein freier R-Modul mit endlichen Rang $n \geq 0$. Es sei $F' \subseteq F$ ein Untermodul. Zeigen Sie, dass F' frei vom Rang $r \leq n$ ist.

Bemerkung. Mithilfe des Auswahlaxioms (in Form des Wohlordnungssatzes) verallgemeinert sich Übung 51 auf freie Moduln beliebigen Rangs.

Lösung 51.

Es genügt den Fall $F = R^n$ für $n \geq 0$ zu betrachten. Wir zeigen die Aussage per Induktion über n. Für $n = 0$ ist die Aussage klar.

Für $n = 1$ sei $\mathfrak{a} \subseteq R$ ein Untermodul, also ein Ideal. Für $\mathfrak{a} = 0$ ist die Aussage klar, wir beschränken uns also auf den Fall $\mathfrak{a} \neq 0$. Es ist $\mathfrak{a}$ ein Hauptideal, also $\mathfrak{a} = (a)$ für ein $a \in \mathfrak{a}$, und nach Annahme gilt $a \neq 0$. Die Teilmenge $\{a\} \subseteq \mathfrak{a}$ ist linear unabhängig, denn die Abbildung $R \to \mathfrak{a}$, $r \mapsto ra$ ist injektiv, da R ein Integritätsbereich ist und $a \neq 0$ gilt. Also ist $\{a\}$ eine Basis von $\mathfrak{a}$, und $\mathfrak{a}$ somit frei vom Rang 1.

Es sei nun $n \geq 2$ und die Aussage gelte für alle kleineren Ränge. Durch die Inklusion $i \colon R^{n-1} \to R^n$, $(x_1, \ldots, x_{n-1}) \mapsto (x_1, \ldots, x_{n-1}, 0)$ und die Projektion $p \colon R^n \to R$, $(x_1, \ldots, x_n) \mapsto x_n$ erhalten wir eine kurze exakte Sequenz $0 \to R^{n-1} \xrightarrow{i} R^n \xrightarrow{p} R \to 0$.

Ist $F' \subseteq F$ ein Untermodul, so schränkt sich diese kurze exakte Sequenz zu einer kurzen exakten Sequenz

$$0 \to i^{-1}(F') \xrightarrow{i'} F' \xrightarrow{p'} p(F') \to 0 \tag{9}$$

ein, wobei i' und p' die entsprechenden Einschränkungen von i und p bezeichnen (siehe Übung 50). Dabei sind $i^{-1}(F') \subseteq R^{n-1}$ und $p(F') \subseteq R$ Untermoduln, und somit nach Induktionsannahme frei vom Rang $\leq n-1$ und ≤ 1. Da $p(F')$ frei ist, spaltet die Sequenz (9); inbesondere ist deshalb $F' \cong i^{-1}(F') \oplus p(F')$. Somit ist F' frei von Rang $\leq n-1+1 = n$.

Übung 52.
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 52.
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 $F \coloneqq \varphi^{-1}(N)$ 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 (siehe Übung 51). Insbesondere ist F endlich erzeugt. Somit ist auch $N = \varphi(F)$ endlich erzeugt.

Übung 53.
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 53.
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 $m_i \coloneqq f(n_i) \in M$; 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 $g(m) = r_{s+1}p_{s+1} + \cdots + r_t p_t$ für passende $r_{s+1}, \dots, r_t \in R$. Es sei $m' \coloneqq r_{s+1}m_{s+1} + \cdots + r_t m_t \in M$. Es gilt
$$g(m') = r_{s+1}g(m_{s+1}) + \cdots + r_t g(m_t) = r_{s+1}p_{s+1} + \cdots + r_t p_t = g(m)$$
   und somit $m - m' \in \ker g = \operatorname{im} N$. Es sei $n \in N$ mit $f(n) = m - m'$. Dann gilt $n = r_1 n_1 + \cdots + r_s n_s$ für passende $r_1, \dots, r_s \in R$, und somit
$$m - m' = f(n) = r_1 f(n_1) + \cdots + r_s f(n_s) = r_1 m_1 + \cdots + r_s m_s.$$
   Ingesamt erhalten wir, dass
$$m = m - m' + m' = r_1 m_1 + \cdots + r_s m_s + r_{s+1} m_{s+1} + \cdots + r_t m_t.$$

Übung 54. *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 54.
Der Vollständigkeit halber geben wir mehr Implikationen an, als notwendig sind.
(1 $\implies$ 2) Es sei
$$N_0 \subseteq N_1 \subseteq N_2 \subseteq N_3 \subseteq N_4 \subseteq \dots \tag{10}$$
eine aufsteigende Kette von Untermoduln von M. Dann ist $N \coloneqq \bigcup_{i\geq 0} N_i$ 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 (10).
(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 $N_0 \coloneqq 0$. 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 $N_{i+1} \coloneqq N_i + \langle f \rangle_R$, 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 $\mathcal{S} \coloneqq \{N_i \mid i \in I\}$ 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 $N'' \coloneqq N' + \langle f \rangle_R$ ein endlich erzeugter Untermodul von N, also ein Element von $\mathcal{S}$, mit $N' \subseteq N''$, was der Maximalität von N' widerspricht. Also muss bereits $N = N'$, und N somit endlich erzeugt sein.

Übung 55.

Es sei R ein Ring.

1. Es sei $0 \to N \to M \to P \to 0$ eine kurze exakte Sequenz von R-Moduln. Zeigen Sie, dass M genau dann noethersch ist, wenn N und P beide noethersch sind.
2. Folgern Sie, dass für alle noetherschen R-Moduln $M_1, \ldots, M_s$ auch $M_1 \oplus \cdots \oplus M_s$ noethersch ist.

Es sei nun R zusätzlich noethersch.

3. Folgern Sie, dass inbesondere R^n für alle $n \geq 0$ noethersch ist, falls R noethersch ist.
4. Folgern Sie, dass jeder endlich erzeugte R-Modul noethersch ist, falls R noethersch ist.

Übung 56.

1. Wir bezeichnen die Abbildungen mit $0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0$.

   Es sei zunächst M noethersch, d.h. jeder Untermodul von M sei endlich erzeugt.

   Dann ist auch der Untermodul $f(N) \subseteq M$ noethersch, denn jeder Untermodul von $f(N)$ ist auch ein Untermodul von M, und somit endlich erzeugt. Wegen der Injektivität von f gilt $N \cong f(N)$, weshalb auch N noethersch ist.

   Ist $P' \subseteq P$ ein Untermodul, so ist $g^{-1}(P') \subseteq M$ ein Untermodul, und somit endlich erzeugt. Damit ist auch $g(g^{-1}(P'))$ endlich erzeugt, und wegen der Surjektivität von g gilt $g(g^{-1}(P')) = P'$. Somit ist jeder Untermodul von P endlich erzeugt, also P noethersch.

   Es seien nun N und P noethersch. Ist $M' \subseteq M$ ein Untermodul, so schränkt die kurze exakte Sequenz $0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0$ zu einer kurzen exakten Sequenz

   $$0 \to f^{-1}(M') \xrightarrow{f'} M' \xrightarrow{g'} g(M') \to 0 \tag{11}$$

   ein, wobei f' und g' die entsprechenden Einschränkungen von f und g bezeichnen (siehe Übung 50). Nach Annahme sind die Untermoduln $f^{-1}(M') \subseteq N$ und $g(M') \subseteq P$ endlich erzeugt. In (11) sind also die beiden äußeren Terme endlich erzeugt; somit ist auch der mittlere Term, also M', endlich erzeugt (siehe Übung 53).

2. Dank Induktion genügt es zu zeigen, dass für je zwei noethersche Moduln M und N auch $M \oplus N$ noethersch ist. Dies ergibt sich aus dem vorherigen Teil der Aufgabe mithilfe der kurzen exakten Sequenz $0 \to M \xrightarrow{i} M \oplus N \xrightarrow{p} N \to 0$, wobei $i\colon M \to M \oplus N$, $m \mapsto (m, 0)$ die kanonische Inklusion bezeichnet und $p\colon M \oplus N \to N$, $(m, n) \mapsto n$ die kanonische Projektion.

3. Da R noethersch ist, ist nach dem vorherigen Aufgabenteil auch $R^n = R \oplus \cdots \oplus R$ wieder noethersch.

4. Ist M ein R-Modul mit endlichen Erzeugendensystem $\{m_1, \ldots, m_n\} \subseteq M$, so ist der eindeutige Modulhomomorphismus $\varphi\colon R^n \to M$ mit $\varphi(e_i) = m_i$ für alle $i = 1, \ldots, n$ (also $\varphi(x_1, \ldots, x_n) = x_1 m_1 + \cdots + x_n m_n$) bereits surjektiv. Wir erhalten somit eine kurze exakte Sequenz $0 \to \ker \varphi \xrightarrow{i} R^n \xrightarrow{\varphi} M \to 0$, wobei $i\colon \ker \varphi \to R^n$ die Inklusion ist. Da R^n nach dem vorherigen Aufgabenteil noethersch ist, ist nach dem ersten Aufgabenteil auch M noethersch.

Übung 57.
Es sei R ein Ring und M ein noetherscher R-Modul. Zeigen Sie, dass jeder surjektive Endomorphismus $f\colon M \to M$ bereits ein Isomorphismus ist.

Bemerkung. Ist R ein kommutativer Ring, so lässt sich Übung 57 dazu verallgemeinern, dass jeder surjektive Endomorphismus $M \to M$ eines endlich erzeugten R-Moduls bereits ein Isomorphismus ist: Mithilfe von Lokalisierungen und Nakayamas Lemma lässt sich diese allgemeine Aussage auf den Fall zurückführen, dass R ein Körper ist, und für Körper ist die Aussage aus der Linearen Algebra bekannt.

Lösung 57.
Da M noethersch ist stabilisiert die Kette

$$0 = \ker f^0 \subseteq \ker f \subseteq \ker f^2 \subseteq \ker f^3 \subseteq \ker f^4 \subseteq \ldots ,$$

d.h. es gibt $n \geq 1$ mit $\ker f^n = \ker f^k$ für alle $k \geq n$. Inbesondere gilt $\ker f^n = \ker f^{2n}$. Für $m \in \ker f^n$ gibt es wegen der Surjektivität von f ein $m' \in M$ mit $m = f^n(m')$. Dann gilt $0 = f^n(m) = f^{2n}(m')$, also $m' \in \ker f^{2n} = \ker f^n$. Deshalb ist bereits $m = f^n(m) = 0$. Das zeigt die Gleichheit $\ker f^n = 0$, und da $\ker f \subseteq \ker f^n$ somit auch, dass $\ker f = 0$ gilt. Also ist f injektiv, und somit bereits ein Isomorphismus.

Übung 58.
Es sei R ein Ring und F ein freier R-Modul mit Basis $(b_i)_{i \in I}$. Zeigen Sie, dass es für jeden R-Modul M und jede Familie $(m_i)_{i \in I}$ von Elementen $m_i \in M$ einen eindeutigen Homomorphismus von R-Moduln $\varphi\colon F \to M$ gibt, so dass $\varphi(b_i) = m_i$ für alle $i \in I$ gilt.

Lösung 58.

Wir zeigen zunächst die Eindeutigkeit: Hierfür sei $\varphi\colon F \to M$ ein Homomorphismen mit $\varphi(b_i) = m_i$ für alle $i \in I$. Jedes $x \in F$ lässt sich als Linearkombination $x = \sum_{i\in I} r_i b_i$ mit $r_i = 0$ für fast alle $i \in I$ schreiben, da die Familie $(b_i)_{i\in I}$ ein Erzeugendensystem von F ist. Deshalb gilt

$$\varphi(x) = \varphi\left(\sum_{i\in I} r_i b_i\right) = \sum_{i\in I} r_i \varphi(b_i) = \sum_{i\in I} r_i m_i.$$

Also ist φ bereits eindeutig bestimmt.

Nun zur Existenz: Für jedes $x \in F$ ist die Darstellung $x = \sum_{i\in I} r_i b_i$ mit $r_i = 0$ für fast alle $i \in I$ eindeutig, da die Familie $(b_i)_{i\in I}$ linear unabhängig ist. Daher ist der Ausdruck $\varphi(x) \coloneqq \sum_{i\in I} r_i m_i$ wohldefiniert, und liefert eine Funktion $\varphi\colon F \to M$. Ist $r \in R$ und sind $x, y \in F$ mit $x = \sum_{i\in I} r_i b_i$ und $y = \sum_{i\in I} s_i b_i$, so gelten $rx = \sum_{i\in I} r r_i b_i$ und $x + y = \sum_{i\in I}(r_i + s_i) b_i$. Deshalb gilt

$$\varphi(rx) = \varphi\left(\sum_{i\in I} r r_i b_i\right) = \sum_{i\in I} r r_i m_i = r \sum_{i\in I} r_i m_i = r\varphi\left(\sum_{i\in I} r_i b_i\right) = r\varphi(x)$$

und

$$\varphi(x + y) = \sum_{i\in I}(r_i + s_i) b_i = \left(\sum_{i\in I} r_i b_i\right) + \left(\sum_{i\in I} s_i b_i\right) = \varphi(x) + \varphi(y).$$

Also ist φ ein Modulhomomorphismus.

Übung 59.

1. Geben Sie für einen passenden kommutativen Ring R eine kurze exakte Sequenz von R-Moduln $0 \to N \to M \to P \to 0$ an, die nicht spaltet.

2. Es sei R ein 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.

Lösung 59.

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 60.

Es sei R ein Ring und $\{N_i \xrightarrow{f_i} M_i \xrightarrow{g_i} P_i\}_{i\in I}$ eine Familie von exakten Sequenzen von R-Moduln.

1. Zeigen Sie, dass auch die induzierte Sequenz
$$\prod_{i\in I} N_i \xrightarrow{f} \prod_{i\in I} M_i \xrightarrow{g} \prod_{i\in I} P_i$$
exakt ist, wobei f und g durch $f((n_i)_{i\in I}) = (f(n_i))_{i\in I}$ für alle $(n_i)_{i\in I} \in \prod_{i\in I} N_i$ und $g((m_i)) = (g(m_i))_{i\in I}$ für alle $(m_i)_{i\in I} \in \prod_{i\in I} M_i$ gegeben sind.
2. Entscheiden Sie, ob die Aussage auch gilt, wenn man das Produkt $\prod_{i\in I}$ jeweils durch die direkte Summe $\bigoplus_{i\in I}$ ersetzt.

Lösung 60.

1. Es gilt $g \circ f = (g_i)_{i\in I} \circ (f_i)_{i\in I} = (g_i \circ f_i)_{i\in I} = 0$, da $g_i \circ f_i = 0$ für alle $i \in I$. Also ist $\operatorname{im} f \subseteq \ker g$.

   Ist andererseits $(m_i)_{i\in I} \in \ker g$, so gilt $0 = g((m_i)_{i\in i}) = (g(m_i))_{i\in I}$, also $g(m_i) = 0$ für alle $i \in I$. Dann ist $m_i \in \ker g_i = \operatorname{im} f_i$ für alle $i \in I$, weshalb es für jedes $i \in I$ ein $n_i \in N_i$ mit $f_i(n_i) = m_i$ gibt. Für $n := (n_i)_{i\in I} \in \prod_{i\in I} N_i$ gilt dann $f(n) = f((n_i)_{i\in I}) = (f(n_i))_{i\in I} = (m_i)_{i\in I} = m$, weshalb $m \in \operatorname{im} f$. Das zeigt, dass $\ker g \subseteq \operatorname{im} f$.
2. Die Aussage gilt auch weiterhin. Der obige Beweis muss nur bei der Wahl der n_i etwas angepasst werden: Damit $(n_i) \in \bigoplus_{i\in I} N_i$ gilt, muss $n_i = 0$ für fast alle $i \in I$ gelten. Da aber ohnehin $m_i = 0$ für fast alle $i \in I$ gilt, lassen sich fast alle n_i als 0 wählen.

Übung 61.

Es sei R ein kommutativer Ring.

1. Zeigen Sie für jedes Ideal $I \subseteq R$ die Gleichheit $\operatorname{Ann}(R/I) = I$.
2. Zeigen Sie für jeden freien R-Modul F mit $F \neq 0$, dass $\operatorname{Ann}(F) = 0$.

Es sei nun zusätzlich $R \neq 0$.

3. Folgern Sie, dass R genau dann ein Körper ist, wenn jeder endlich erzeugte R-Modul frei ist.

Lösung 61.

1. Für alle $x \in I$ und $\overline{y} \in R/I$ gilt $xy \in I$ und somit $\overline{xy} = \overline{xy} = 0$. Deshalb gilt $I \subseteq \operatorname{Ann}(R/I)$. Für jedes $x \in \operatorname{Ann}(R/I)$ gilt $0 = x \cdot \overline{1} = \overline{x}$ und somit $x \in I$. Deshalb ist auch $\operatorname{Ann}(R/I) \subseteq I$.

2. Da F frei ist, besitzt F eine Basis; da $F \neq 0$ gilt, ist diese nicht leer. Es gibt daher ein Element $m \in F$, so dass $\{m\} \subseteq F$ linear unabhängig ist. Dann gilt $xm \neq 0$ für alle $x \in R$ mit $x \neq 0$, und deshalb $x \notin \operatorname{Ann}(F)$.

3. Ist R ein Körper, so besitzt jeder endlich erzeugte erzugte R-Modul, also endlicher erzeugte R-Vektorraum, bekanntermaßen eine Basis. Ist andererseits R kein Körper, so gibt es ein Ideal $I \subseteq R$ mit $I \neq 0, R$ (siehe Übung 78). Dann ist $M := R/I$ ein endlich erzeugter R-Modul mit $M \neq 0$ (da $I \neq R$) sowie $\operatorname{Ann}(R/I) = I \neq 0$. Nach dem vorherigen Aufgabenteil ist M nicht frei.

Übung 62.

Es sei R ein Ring und $0 \to N \to M \to P \to 0$ eine kurze exakte Sequenz von R-Moduln.

1. Es sei zunächst R ein Hauptidealbereich und $p \in R$ prim. Zeigen Sie, dass M genau dann p-primär ist, wenn N und P beide p-primär sind.

2. Zeigen Sie allgemeiner, dass $\sqrt{\operatorname{Ann}(M)} = \sqrt{\operatorname{Ann}(N)} \cap \sqrt{\operatorname{Ann}(P)}$. (Dabei gilt die Gleichheit $\sqrt{\operatorname{Ann}(N)} \cap \sqrt{\operatorname{Ann}(P)} = \sqrt{\operatorname{Ann}(N) \cap \operatorname{Ann}(P)}$, siehe Übung 9.

Lösung 62.

Wir bezeichnen die gegebene kurze exakte Sequenz mit $0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0$.

1. Es sei zunächst M p-primär. Dann ist auch der Untermodul $f(N) \subseteq M$ p-primär, und da f eine Isomorphie $N \cong f(N)$ liefert, damit auch N p-primär. Für $x \in P$ gibt es $x' \in M$ mit $g(x') = x$; da M p-primär ist, gibt es ein $k \geq 0$ mit $p^k x' = 0$ und somit auch $p^k x = p^k g(x') = g(p^k x') = g(0) = 0$. Also ist auch P p-primär.

   Es seien nun N und P beide p-primär. Für $m \in M$ ist $g(m) \in P$, es gibt also $k_2 \geq 0$ mit $p^{k_2} g(m) = 0$. Dann gilt $g(p^{k_2} m) = p^{k_2} g(m) = 0$ und somit $p^{k_2} m \in \ker g = \operatorname{im} f$. Es gibt also ein $n \in N$ mit $p^{k_2} m = f(n)$. Da N p-primär ist, gibt es ein $k_1 \geq 0$ mit $p^{k_1} n = 0$. Ingesamt erhalten wir, dass

   $$p^{k_1+k_2} m = p^{k_1} p^{k_2} m = p^{k_1} f(n) = f(p^{k_1} n) = f(0) = 0.$$

   Das zeigt, dass M p-primär ist.

2. Für $x \in R$ gilt genau dann $x \in \sqrt{\operatorname{Ann}(M)}$, wenn es $k \geq 0$ mit $x^k \in \operatorname{Ann}(M)$ gibt, also genau dann, wenn es $k \geq 0$ mit $x^k M = 0$ gibt. Es gilt also genau dann $x \in \sqrt{\operatorname{Ann}(M)}$, wenn M „x-primär“ ist. Ersetzt man in der obigen Argumentation p durch x, so erhält man deshalb, dass genau dann $x \in \sqrt{\operatorname{Ann}(M)}$ gilt, wenn $x \in \sqrt{\operatorname{Ann}(N)}$ und $x \in \sqrt{\operatorname{Ann}(P)}$ gelten.

Übung 63.
Es sei M ein R-Modul.

1. Zeigen Sie, dass $\mathrm{Ann}(\langle m\rangle_R) = \mathrm{Ann}(m)$ für jedes $m \in M$.
2. Zeigen Sie, dass $\mathrm{Ann}(\sum_{i\in I} M_i) = \bigcap_{i\in I} \mathrm{Ann}(M_i)$ für jede Familie $(M_i)_{i\in I}$ von Untermoduln $M_i \subseteq M$.
3. Folgern Sie, dass $\mathrm{Ann}(\langle m_i \mid i \in I\rangle_R) = \bigcap_{i\in I} \mathrm{Ann}(m_i)$ für jede Familie $(m_i)_{i\in I}$ von Elementen $m_i \in M$, und dass $\mathrm{Ann}(M) = \bigcap_{m\in M} \mathrm{Ann}(m)$.
4. Zeigen Sie, dass $\sum_{i\in I} \mathrm{Ann}(M_i) \subseteq \mathrm{Ann}(\bigcap_{i\in I} M_i)$ für jede Familie $(M_i)_{i\in I}$ von Untermoduln $M_i \subseteq M$.
5. Geben Sie ein Beispiel an, in dem die obige Inklusion strikt ist.

Lösung 63.
1. Aus der Inklusion $\{m\} \subseteq \langle m\rangle_R$ folgt die Inklusion $\mathrm{Ann}(\langle M\rangle_R) \subseteq \mathrm{Ann}(m)$. Ist andererseits $x \in \mathrm{Ann}(m)$, so gilt $xm = 0$, und somit auch $x(rm) = r(xm) = 0$ für alle $r \in R$, also $xm' = 0$ für alle $m' \in \{rm \mid r \in R\} = \langle m\rangle_R$.
2. Für jedes $j \in J$ folgt sich aus $M_j \subseteq \sum_{i\in I} M_i$ die Inklusion $\mathrm{Ann}(\sum_{i\in I} M_i) \subseteq \mathrm{Ann}(M_j)$, und somit insgesamt die Inklusion $\mathrm{Ann}(\sum_{i\in I} M_i) \subseteq \bigcap_{i\in I} \mathrm{Ann}(M_i)$. Gilt andererseits $x \in \bigcap_{i\in I} \mathrm{Ann}(M_i)$, so gilt $xM_i = 0$ für alle $i \in I$, also $xm_i = 0$ für alle $i \in I$ und $m_i \in M_i$. Da jedes $m \in \sum_{i\in I} M_i$ eine endliche Summe solcher m_i ist, gilt bereits $xm = 0$ für alle $m \in \sum_{i\in I} M_i$, und somit $x \in \mathrm{Ann}(\sum_{i\in I} M_i)$. Somit gilt auch $\bigcap_{i\in I} \mathrm{Ann}(M_i) \subseteq \mathrm{Ann}(\sum_{i\in I} M_i)$.
3. Es gilt die Gleichungskette
$$\mathrm{Ann}(\langle m_i \mid i \in I\rangle_R) = \mathrm{Ann}\left(\sum_{i\in I} \langle m_i\rangle_R\right) = \bigcap_{i\in I} \mathrm{Ann}(\langle m_i\rangle_R) = \bigcap_{i\in I} \mathrm{Ann}(m_i)$$
und somit insbesondere $\mathrm{Ann}(M) = \mathrm{Ann}(\sum_{m\in M} \langle m\rangle_R) = \bigcap_{m\in M} \mathrm{Ann}(m)$.
4. Es gilt genau dann $\sum_{i\in I} \mathrm{Ann}(M_i) \subseteq \mathrm{Ann}(\bigcap_{i\in I} M_i)$, wenn $\mathrm{Ann}(M_j) \subseteq \mathrm{Ann}(\bigcap_{i\in I} M_i)$ für alle $j \in I$. Für jedes $j \in I$ ergibt sich diese Inklusion aus der Inklusion $\bigcap_{i\in I} M_i \subseteq M_j$.
5. Für $R \neq 0$ betrachte man $M = R \oplus R$ mit den Untermoduln $M_1 = R \oplus 0$ und $M_2 = 0 \oplus R$. Dann gilt $M_1 \cong M_2 \cong R$ und somit $\mathrm{Ann}(M_1) = \mathrm{Ann}(M_2) = \mathrm{Ann}(R) = 0$. Deshalb gilt $\mathrm{Ann}(M_1) + \mathrm{Ann}(M_2) = 0$. Andererseits gilt $M_1 \cap M_2 = 0$ und somit $\mathrm{Ann}(M_1 \cap M_2) = \mathrm{Ann}(0) = R \neq 0$.

Übung 64.
Es sei R ein kommutativer Ring und $I, J \subseteq R$ seien zwei Ideale, so dass $R/I \cong R/J$ als R-Moduln. Zeigen Sie, dass bereits $I = J$. (*Hinweis*: Betrachten Sie Annihilatoren.)

Lösung 64.
Für jedes Ideal $K \subseteq R$ gilt $\operatorname{Ann}(R/K) = K$ (siehe Übung 61), und somit gilt

$$I = \operatorname{Ann}(R/I) = \operatorname{Ann}(R/J) = J.$$

Übung 65. *Existenz der Hauptraumzerlegung*
Es sei K ein Körper, V ein K-Vektorraum und $f\colon V \to V$ ein Endomorphismus.

1. Zeigen Sie für je zwei teilerfremde Polynome $p, q \in K[T]$ die Gleichheit
$$\ker (pq)(f) = \ker p(f) \oplus \ker q(f).$$
2. Folgern Sie für alle paarweise teilerfremden Polynome $p_1, \dots, p_n \in K[T]$ die Gleichheit
$$\ker (p_1 \cdots p_n)(f) = \ker p_1(f) \oplus \cdots \oplus \ker p_n(f).$$

Es sei nun K algebraisch abgeschlossen und V endlichdimensional.

3. Zeigen Sie, dass V in die Summe der Haupträume von f ist.

Lösung 65.
1. Da p und q teilerfremd sind, gibt es $a, b \in K[T]$ mit $ap + bq = 1$. Durch Einsetzen von f ergibt sich, dass $a(f)p(f) + b(f)g(f) = \mathrm{id}_V$. Für $v \in \ker p(f) \cap \ker q(f)$ gilt deshalb
$$0 = a(f)(\underbrace{p(f)(v)}_{=0}) + b(f)(\underbrace{q(f)(v)}_{=0}) = (a(f)p(f) + b(f)q(f))(v) = \mathrm{id}_V(v) = v.$$
Also ist $\ker p(f) \cap \ker q(f) = 0$. Für $v \in \ker (pq)(f)$ gilt andererseits
$$v = \mathrm{id}_V(v) = (a(f)p(f) + b(f)q(f))(v) = \underbrace{(a(f)p(f))(v)}_{=:v_2} + \underbrace{(b(f)q(v))(v)}_{=:v_1}$$
Dabei gilt $v_1 \in \ker p(f)$, da
$$\begin{aligned} p(f)(v_1) &= (p(f)b(f)q(f))(v) = (b(f)p(f)q(f))(v) \\ &= (b(f)(pq)(f))(v) = b(f)(\underbrace{(pq)(f)(v)}_{=0}) = 0. \end{aligned}$$
Analog gilt auch $v_2 \in \ker q(f)$. Also gilt auch $\ker (pq)(f) = \ker p(f) + \ker q(f)$.

2. Wir zeigen die Aussage per Induktion über n. Für $n = 1$ ist die Aussage klar, und für $n = 2$ wurde sie im vorherigen Teil der Aussage gezeigt. Es sei also $n \geq 3$; da $f_1, \ldots, f_n$ paarweise teilerfremd sind, sind auch die beiden Polynome $f_1 \cdots f_{n-1}$ und f_n teilerfremd. Nach Induktionsvoraussetzung gilt deshalb

$$\ker (p_1 \cdots p_n)(f) = \ker (p_1 \cdots p_{n-1} \cdot p_n)(f) = \ker (p_1 \cdots p_{n-1})(f) \oplus \ker p_n(f). \quad (12)$$

Da $f_1, \ldots, f_n$ paarweise teilerfremd sind, sind es auch $f_1, \ldots, f_{n-1}$. Nach Induktionsvoraussetzung gilt daher auch

$$\ker (p_1 \cdots p_{n-1})(f) = \ker p_1(f) \oplus \cdots \oplus \ker p_{n-1}(f). \quad (13)$$

Zusammenfügen von (12) und (13) ergibt die Aussage.

3. Es sei $p \in K[T]$ das charakteristische Polynom von f. Da K algebraisch abgeschlossen ist zerfällt p in Linearfaktoren, also $p(T) = (T - \lambda_1)^{n_1} \cdots (T - \lambda_s^{n_s})$ für $n_1, \ldots, n_s \geq 0$ und paarweise verschiedene $\lambda_1, \ldots, \lambda_s \in K$. Die Polynome $(T - \lambda_1)^{n_1}, \ldots, (T - \lambda_s)^{n_s}$ sind paarweise teilerfremd, und somit gilt nach dem vorherigen Aussagenteil

$$\ker p(f) = \ker(f - \lambda_1)^{n_1} \oplus \cdots \oplus \ker(f - \lambda_s)^{n_s}.$$

Nach dem Satz von Cayley-Hamilton gilt dabei $p(f) = 0$ und somit $\ker p(f) = V$.

Übung 66. *Torsionsuntermoduln*
Es sei R ein Integritätsbereich mit Quotientenkörper K.

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 $T(M)$ der Kern der kanonischen Abbildung $M \to M_K$, $m \mapsto m/1$ ist.
3. Zeigen Sie für jeden R-Moduln M, dass $T(M \oplus N) = T(M) \oplus T(N)$ für alle R-Moduln M und N.
4. Zeigen Sie, dass jeder freie R-Modul torsionsfrei ist.
5. Zeigen Sie für jeden R-Moduln M, dass $M/T(M)$ torsionsfrei ist.
6. 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 $T(f)\colon T(M) \to T(N)$, $m \mapsto f(m)$.

7. 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 $N \xrightarrow{f} M \xrightarrow{g} P$.

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

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

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

Lösung 66.

1. Es ist $T(M) = \{m \in M \mid rm = 0 \text{ für ein } r \in R \text{ mit } r \neq 0\}$. Es gilt $0 \in M$, da $1 \cdot 0 = 0$.

   Für $m_1, m_2 \in T(M)$ gibt es $r_1, r_2 \in R$ mit $r_1, r_2 \neq 0$, so dass $r_1 m_1 = r_2 m_2 = 0$. Dann gilt auch $(r_1 r_2)(m_1 + m_2) = r_2 r_1 m_1 + r_1 r_2 m_2 = 0$, wobei $r_1 r_2 \neq 0$, da R ein Integritätsbereich ist. Also gilt auch $m_1, m_2 \in M$.

   Für $m \in T(M)$ gibt es $r \in R$ mit $rm = 0$ und $r \neq 0$. Für jedes $r' \in R$ ist dann auch $r(r'm) = r'(rm) = 0$, und somit $r'm \in T(M)$.

2. Es ist K die Lokalisierung von R an der multiplikativen Menge $S = R \setminus \{0\}$. Für die kanonische Abbildung $i\colon M \to M_K, m \mapsto m/1$ gilt deshalb

$$m \in \ker i \iff \frac{m}{1} = \frac{0}{1} \iff \exists s \in S : s \cdot m = 0 \iff m \in T(M).$$

3. Für $(m, n) \in T(M)$ gibt es $r \in R$ mit $r \neq 0$ und $0 = r(m, n) = (rm, rn)$. Dann gilt $rm = 0$ un $rn = 0$, und wegen $r \neq 0$ gelten somit $m \in T(M)$ und $n \in T(N)$. Also gilt $T(M \oplus N) \subseteq T(M) \oplus T(N)$.

   Für $(m, n) \in T(M) \oplus T(N)$ gibt es $r_1, r_2 \in R$ mit $r_1, r_2 \neq 0$ und $r_1 m = 0$ und $r_2 n = 0$. Dann gelten $(r_1 r_2)(m, n) = (r_2, r_1 m, r_1 r_2 n) = (0, 0)$, und da R ein Integritätsbereich ist, gilt $r_1 r_2 \neq 0$. Also ist $(m, n) \in T(M \oplus N)$, und somit $T(M) \oplus T(N) \subseteq T(M \oplus N)$.

4. Es sei F ein freier R-Modul mit Basis $(b_i)_{i \in I}$ und $m \in T(F)$. Dann gibt es eine (eindeutige) Darstellung $m = \sum_{i \in I} r_i b_i$ mit $r_i = 0$ für fast alle $i \in I$. Nach Annahme gibt es $r \in R$ mit $r \neq 0$ und $0 = rm = \sum_{i \in I} r r_i b_i$. Wegen der linearen Unabhängigkeit der Familie $(b_i)_{i \in I}$ muss bereits $r r_i = 0$ für alle $i \in I$. Da R ein Integritätsbereich ist folgt zusammen mit $r \neq 0$, dass $r_i = 0$ für alle $i \in I$. Somit ist bereits $m = \sum_{i \in I} r_i b_i = 0$.

5. Es sei $\overline{m} \in T(M/T(M))$. Dann gibt es $r_2 \in R$ mit $r_2 \neq 0$ und $0 = r_2 \overline{m} = \overline{r_2 m}$, also $r_1 m \in T(M)$. Dann gibt es wiederum $r_1 \in R$ mit $r_1 \neq 0$ und $r_1 r_2 m = 0$. Da R ein Integritätsbereich ist, gilt dabei $r_1 r_2 \neq 0$. Deshalb gilt bereits $m \in T(M)$ und somit $\overline{m} = 0$.

6. Es sei $m \in T(M)$. Dann gibt es $r \in R$ mit $r \neq 0$ und $rm = 0$. Dann gilt auch $rf(m) = f(rm) = f(0) = 0$ und somit $f(m) \in T(N)$.

7. Dass $T(\mathrm{id}_M) = \mathrm{id}_{T(M)}$ gilt ist klar, und dass $T(g \circ f) = T(g) \circ T(f)$ gilt, folgt aus der Veträglichkeit von Komposition und Restriktion.

8. Wegen der Injektivität von f ist auch $T(f)$ injektiv, die Sequenze also exakt an $T(N)$. Für die Exaktheit an $T(M)$ bemerken wir zunächst, dass $T(g)\circ T(f) = T(g\circ f) = T(0) = 0$, und somit $\operatorname{im} T(f) \subseteq \ker T(g)$. Ist andererseits $m \in \ker T(g) = \ker g \cap T(M)$, so ist $m \in \ker g = \operatorname{im} f$, weshalb es ein $n \in N$ mit $m = f(n)$. Da $m \in T(M)$ gilt, gibt es $r \in R$ mit $r \neq 0$ und $0 = rm = rf(n) = f(rn)$. Wegen der Injektivität von f gilt bereits $rn = 0$ und somit $n \in T(N)$. Also gilt bereits $m = f(n) = T(f)(n) \in \operatorname{im} T(f)$ und somit $\ker T(g) \subseteq \operatorname{im} T(f)$.

9. Wir betrachten das folgende Gegenbeispiel von $\mathbb{Z}-$Moduln: Die kanonische Projektion $p\colon \mathbb{Z} \to \mathbb{Z}/2$, $n \mapsto \overline{n}$ ist zwar surjektiv, die induzierte Abbildung

$$0 = T(\mathbb{Z}) \xrightarrow{T(p)} T(\mathbb{Z}/2) = \mathbb{Z}/2$$

kann es aber nicht sein. (Dass $T(\mathbb{Z}) = 0$ folgt daraus, dass $\mathbb{Z}$ als freier $\mathbb{Z}$-Modul torsionfrei ist.)

Übung 67.
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 $M \cong R/\operatorname{Ann}(M)$ 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 67.
(1 $\implies$ 2) Es sei $m \in M$ mit $M = \langle m\rangle_R$. Dann gilt

$$\operatorname{Ann}(M) = \operatorname{Ann}(\langle m\rangle_R) = \operatorname{Ann}(m) = \{r \in R \mid rm = 0\}.$$

Für den surjektive Homomorphismus von R-Moduln

$$\varphi\colon R \to M, \quad r \mapsto rm$$

gilt deshalb $\ker\varphi = \operatorname{Ann}(M)$. 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 $I = \operatorname{Ann}(M)$.
(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 68. *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 68.
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 69. *Kürzungsregeln bis auf Isomorphie*
Geben Sie einen jeweils passenden kommutativen Ring R Beispiele für R-Moduln M_1 und M_2, sowie Untermoduln $N_1 \subseteq M_1$ und $N_2 \subseteq M_2$, so dass die folgenden Bedingungen erfüllt sind:

1. Es gilt $M_1 \cong M_2$ und $N_1 \cong N_2$, aber $M_1/N_1 \ncong M_2/N_2$.
2. Es gilt $M_1 \cong M_2$ und $M_1/N_1 \cong M_2/N_2$, aber $N_1 \ncong N_2$.
3. Es gilt $M_1/N_1 \cong M_2/N_2$ und $N_1 \cong N_2$, aber $M_1 \ncong M_2$.

(*Hinweis*: Betrachten Sie Moduln der Form $\bigoplus_{n\in\mathbb{N}} R$.)

Lösung 69.
Für die ersten beiden Beispiel sei R ein beliebiger kommutativer Ring mit $R \neq 0$.

1. Wir betrachten $M_1 = M_2 = \bigoplus_{n\geq 0} R = R \oplus R \oplus R \oplus \cdots$ und die Untermoduln $N_1 = 0 \oplus \bigoplus_{n\geq 1} R = 0 \oplus R \oplus R \oplus \cdots$ und $N_2 = 0 \oplus 0 \oplus \bigoplus_{n\geq 2} R = 0 \oplus 0 \oplus R \oplus \cdots$; dann gilt $M_1 = M_2 \cong N_1 \cong N_2$, aber
   $$M_1/N_1 \cong R \ncong R^2 \cong M_2/N_2.$$
   (Hier nutzen wir, dass wegen $R \neq 0$ und der Kommutativität von R der Rang eines freien R-Moduln wohldefiniert ist.)

2. Wir betrachten erneut $M_1 = M_2 = \bigoplus_{n\geq 0} R$, dieses Mal mit den jeweiligen Untermoduln $N_1 = R \oplus \bigoplus_{n\geq 1} 0 = R \oplus 0 \oplus 0 \oplus \cdots$ und $N_2 = R \oplus R \oplus \bigoplus_{n\geq 2} 0 = R \oplus R \oplus 0 \oplus 0 \oplus \cdots$; dann gelten $M_1 = M_2$ und

$$M_1/N_1 \cong \bigoplus_{n\geq 1} R \cong \bigoplus_{n\geq 2} R \cong M_2/N_2,$$

aber $N_1 \cong R \ncong R^2 \cong N_2$.

Für das dritte Gegenbeispiel muss R weiter eingeschränkt werden; ist etwa R ein Körper, so folgt aus $N_1 \cong N_2$ und $M_1/N_1 \cong M_2/N_2$, dass bereits

$$\dim M_1 = \dim M_1/N_1 + \dim N_1 = \dim M_2/N_2 + \dim N_2 = \dim M_2,$$

und somit $M_1 \cong M_2$. Wir betrachten daher den Fall $R = \mathbb{Z}$.

3. Es seien $M_1 = \mathbb{Z}/4$, $M_2 = \mathbb{Z}/2 \oplus \mathbb{Z}/2$, $N_1 = \{0, 2\} = 2M_1$ und $N_2 = \mathbb{Z}/2 \oplus 0$. Dann gelten $M_1/N_1 \cong \mathbb{Z}/2 \cong M_2/N_2$ und $N_1 \cong \mathbb{Z}/2 \cong N_2$ aber $M_1 \ncong M_2$.

Übung 70. *Isomorphie von kurzen exakten Sequenzen*
Es sei R ein Ring. Zwei kurze exakte Sequenzen

$$0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0 \quad \text{und} \quad 0 \to N' \xrightarrow{f'} M' \xrightarrow{g'} P' \to 0$$

von R-Moduln heißen *isomorph*, wenn es Isomorphismen $\varphi_N \colon N \to N'$, $\varphi_M \colon M \to M'$ und $\varphi_P \colon P \to P'$ gibt, die das folgende Diagramm zu kommutieren bringen:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{f} & M & \xrightarrow{g} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_N} & & \downarrow{\scriptstyle \varphi_M} & & \downarrow{\scriptstyle \varphi_P} & & \\ 0 & \longrightarrow & N' & \xrightarrow{f'} & M' & \xrightarrow{g'} & P' & \longrightarrow & 0 \end{array}$$

1. Zeigen Sie, dass Isomorphie von kurzen exakten Sequenzen eine Äquivalenzrelation auf der Klasse der kurzen exakten Sequenzen von R-Moduln ist.

2. Es sei $0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0$ eine kurze exakte Sequenz von R-Moduln. Zeigen Sie, dass sich das Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{f} & M & \xrightarrow{g} & P & \longrightarrow & 0 \\ & & & & \| & & & & \\ 0 & \longrightarrow & \operatorname{im} f & \xrightarrow{i} & M & \xrightarrow{p} & P & \longrightarrow & 0 \end{array}$$

zu einem Isomorphismus von kurzen exakten Sequenzen ergänzen lässt. Dabei bezeichnet $i \colon \operatorname{im} f \to M$, $x \mapsto x$ die Inklusion und $p \colon M \to M/\operatorname{im} f$, $x \mapsto \overline{x}$ die kanonische Projektion.

(Mit anderen Worten: Die beiden Zeilen im obigen Diagramm sind isomorphe kurze exakte Sequenzen, und es gibt einen Isomorphismus, dessen mittlerer vertikaler Pfeil die Identität ist.)

Bemerkung. Übung 70 gibt eine formale Begründung der informalen Aussage, dass jede kurze exakte Sequenz von R-Moduln von der Form $0 \to N \to M \to M/N \to 0$ für einen R-Modul M und Untermodul $N \subseteq M$ ist (wobei die Pfeile $N \to M$ und $M \to M/N$ die jeweils kanonischen Homomorphismen sind).

Übung 71. *Zwei Vierer- und ein Fünferlemma*
Es sei R ein Ring und

$$\begin{array}{ccccccccc} M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \xrightarrow{f_3} & M_4 & \xrightarrow{f_4} & M_5 \\ \downarrow{\scriptstyle h_1} & & \downarrow{\scriptstyle h_2} & & \downarrow{\scriptstyle h_3} & & \downarrow{\scriptstyle h_4} & & \downarrow{\scriptstyle h_5} \\ N_1 & \xrightarrow{g_1} & N_2 & \xrightarrow{g_2} & N_3 & \xrightarrow{g_3} & N_4 & \xrightarrow{g_4} & N_5 \end{array}$$

ein kommutatives Diagramm von R-Moduln mit exakten Ze

1. Es sei h_1 surjektiv, und h_2 und h_4 seien injektiv. Zeigen Sie, dass auch h_3 injektiv ist.
2. Es sei h_5 injektiv, und h_2 und h_4 seien surjektiv. Zeigen Sie, dass auch h_3 surjektiv ist.
3. Folgern Sie: Sind h_1, h_2, h_4 und h_5 Isomorphismen, so ist auch h_3 ein Isomorphismus.

3 Gruppentheorie

Übung 72. *Multiple Choice*

1. Für jeden Körper K und jedes $n \geq 1$ ist $C_n(K) \coloneqq \{x \in K \mid x^n = 1\}$ eine zyklische Untergruppe von $K^\times$.

Lösung 72.

1. Die Aussage ist wahr: Dass $C_n(K)$ eine Untergruppe von $K^\times$ ist, ergibt sich durch direktes Nachrechnen; alternativ erkennt man, dass die Abbildung $K^\times \to K^\times$, $x \mapsto x^n$ ein Gruppenhomomorphismus ist, und $C_n(K)$ ihr Kern ist. Die Gruppe $C_n(K)$ ist endlich, da sie die Nullstellenmenge des Polynoms $X^n - 1 \in K[X]$ ist. Als endliche Untergruppe der multiplikativen Gruppe eines Körpers ist $C_n(K)$ zyklisch.

Übung 73.

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 73.

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 74. *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 74.
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.

Übung 75. *Innere Automorphismen*
Es sei G eine Gruppe.

1. Zeigen Sie, dass für jedes $g \in G$ die Abbildung $c_g \colon G \to G, h \mapsto ghg^{-1}$ ein Gruppenautomorphismus ist.
2. Zeigen Sie, dass die Abbildung $c \colon G \to G, g \mapsto c_g$ ein Gruppenhomomorphismus ist.
3. Zeigen Sie, dass $\ker c = \mathrm{Z}(G)$.
4. Zeigen Sie, dass $\operatorname{Inn} G := \operatorname{im} c$ eine normale Untergruppe von $\operatorname{Aut} G$ ist.

Man bezeichnet $\operatorname{Inn} G$ als die Gruppe der *inneren Automorphismen* von G.

Lösung 75.
1. Für alle $h_1, h_2 \in G$ gilt

$$c_g(h_1 h_2) = g h_1 h_2 g^{-1} = g h_1 g^{-1} g h_2 g^{-1} = c_g(h_1) c_g(h_2),$$

   also ist c_g ein Gruppenhomomorphismus. Für alle $h \in G$ gilt

$$c_g(c_{g^{-1}}(h)) = g g^{-1} h g g^{-1} = h = g^{-1} g h g^{-1} g = c_{g^{-1}}(c_g(h)),$$

   also ist c_g bijektiv mit $c_g^{-1} = c_{g^{-1}}$.
2. Für alle $g_1, g_2 \in G$ gilt

$$c_{g_1 g_2}(h) = (g_1 g_2) h (g_1 g_2)^{-1} = g_1 g_2 h g_2^{-1} g_1^{-1} = c_{g_1}(c_{g_2}(h)) \qquad \text{für alle } h \in G$$

   und somit $c_{g_1 g_2} = c_{g_1} c_{g_2}$.
3. Für $g \in G$ gilt

$$\begin{aligned} g \in \ker c &\iff c_g = \mathrm{id}_G \iff \forall h \in G : c_g(h) = h \\ &\iff \forall h \in G : ghg^{-1} = h \iff \forall h \in G : gh = hg \iff g \in \mathrm{Z}(G). \end{aligned}$$

4. Da c ein Gruppenhomomorphismus ist, ist $\operatorname{Inn} G$ ein Untergruppe von $\operatorname{Aut} G$. Für jedes $\phi \in \operatorname{Aut} G$ und jedes $g \in G$ gilt $\phi c_g \phi^{-1} = c_{\phi(g)}$, denn für alle $h \in G$ gilt

$$(\phi c_g \phi^{-1})(h) = \phi(c_g(\phi^{-1}(h))) = \phi(g\phi^{-1}(h)g^{-1}) = \phi(g)h\phi(g)^{-1} = c_{\phi(g)}(h).$$

Folglich ist $\phi \operatorname{Inn} G \, \phi^{-1} \subseteq \operatorname{im} c$ für alle $\phi \in \operatorname{Aut} G$, also $\operatorname{im} c$ normal in $\operatorname{Aut} G$.

Übung 76.
Es sei G eine Gruppe, die auf einer Menge X vermöge $G \times X \to X$, $(g, x) \mapsto g.x$ wirkt.

1. Definieren Sie die Bahn $G.x$ und den Stabilisator G_x eines Elementes $x \in X$.
2. Zeigen Sie, dass G_x für alle $x \in X$ eine Untergruppe von G ist.
3. Konstruieren Sie für jedes $x \in X$ eine Bijektion $G/G_x \to G.x$.
4. Es seien $x, y \in X$ zwei Elemente mit gleicher G-Bahn. Zeigen Sie, dass die Stabilisatoren G_x und G_y konjugiert zueinander sind.
5. Entscheiden Sie, ob auch die Umkerung der obigen Aussage notwendigerweise gilt.
6. Zeigen Sie, dass X die disjunkte Vereinigung der G-Bahnen ist.

Lösung 76.
1. Es gilt $G.x = \{g.x \mid g \in G\}$, der Stabilisator von x ist $G_x = \{g \in G \mid g.x = x\}$.
2. Es gilt $1 \in G_x$ da $1.x = x$. Für $g_1, g_2 \in G_x$ gilt $(g_1 g_2).x = g_1.(g_2.x) = g_1.x = x$ und somit auch $g_1 g_2 \in G_x$. Für $g \in G$ gilt $g^{-1}.x = g^{-1}.(g.x) = (g^{-1}.g).x = 1.x = x$ und somit auch $g^{-1} \in G_x$. Ingesamt zeigt dies, dass G_x ein Untergruppe von G ist.
3. Die Abbildung $f\colon G \to G.x$, $g \mapsto g.x$ ist surjektiv, und für $g_1, g_2 \in G$ gilt

$$\begin{aligned} f(g_1) = f(g_2) &\iff g_1.x = g_2.x \iff g_2^{-1}.g_1.x = x \\ &\iff (g_2^{-1}g_1).x = x \iff g_2^{-1}g_1 \in G_x \iff g_1 G_x = g_2 G_x, \end{aligned}$$

weshalb f durch eine wohldefinierte Bijektion $\overline{f}\colon G/G_x \to G.x$, $\overline{g} \mapsto g.x$ faktorisiert.
4. Haben x und y die Gleiche G-Bahn, so gibt es $g \in G$ mit $y = g^{-1}.x$. Für alle $h \in G$ gilt dann

$$\begin{aligned} h \in G_y &\iff h.y = y \iff h.g^{-1}.x = g^{-1}.x \\ &\iff g.h.g^{-1}.x = x \iff (ghg^{-1}).x = x \iff ghg^{-1} \in G_x. \end{aligned}$$

Wegen der Bijektivität der Konjugationsabbildung $G \to G$, $h \mapsto ghg^{-1}$ folgt, dass $gG_yg^{-1} = G_x$.

5. Die Umkehrung gilt nicht: Gilt etwa $G = 1$, so gilt $G_x = G$ für alle $x \in X$, aber alle Bahnen sind einelementig. Für $|X| \geq 2$ ergibt dies ein Gegenbeispiel.

   Allgemeiner kann man eine beliebige Gruppe G auf einer Menge X mit $|X| \geq 2$ trivial wirken lassen, d.h. es gelte $g.x = x$ für alle $g \in G$ und $x \in X$. Dann gilt $G_x = G$ für alle $x \in X$ aber alle Bahnen sind einelementig.

6. Es genügt zu zeigen, dass $x \sim y \iff x \in G.y$ eine Äquivalenzrelation auf X definiert, denn dann sind die G-Bahnen genau die Äquivalenzklassen von $\sim$. Da $x = 1.x \in G.x$ ist die Relation reflexiv. Gilt $x \sim y$ so gibt es $g \in G$ mit $x = g.x$; dann gilt auch $y = g^{-1}.x \in G.x$ und somit $y \sim x$. Für $x, y, z \in X$ mit $x \sim y$ und $y \sim z$ gibt es $g, h \in G$ mit $x = g.y$ und $y = h.z$; dann gilt auch $x = g.y = g.h.z = (gh).z \in G.z$ und somit $x \sim z$.

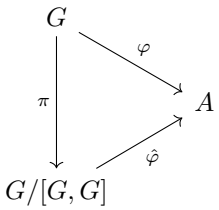
Übung 77.
Es sei G ein Gruppe.

1. Definieren Sie die Kommutatoruntergruppe $[G, G]$ von G.

2. Zeigen Sie, dass $[G, G]$ eine normale Untergruppe von G ist, und dass $G/[G, G]$ abelsch ist.

3. Es sei $N \subseteq G$ eine normale Untergruppe, so dass G/N abelsch ist. Zeigen Sie, dass $N \subseteq [G, G]$.

4. Zeigen Sie, dass $G/[G, G]$ die folgende universelle Eigenschaft hat: Ist A eine abelsche Gruppe und $\varphi\colon G \to A$ ein Gruppenhomomorphismus, so gibt es einen eindeutigen Gruppenhomomorphismus $\hat{\varphi}\colon G/[G, G] \to A$, der das folgende Diagram zum kommutieren bringt:



   Dabei bezeichnet $\pi\colon G \to G/[G, G]$, $g \mapsto \overline{g}$ die kanonische Projektion.

4 Körpertheorie

Übung 78.
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 78.
(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 79.
Es sei K ein algebraisch abgeschlossener Körper. Zeigen Sie, dass K unendlich ist.

Lösung 79.
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 80.
Es sei K ein Körper und $p \in K[T]$ ein Polynom mit $\deg p \in \{2, 3\}$. Zeigen Sie, dass p genau dann irreduzibel ist, wenn p keine Nullstelle hat.

Lösung 80.
Wäre p reduzibel, so gebe $q_1, q_2 \in K[T]$ mit $p = q_1 q_2$ und $\deg q_1, \deg q_2 \geq 1$. Es müsste dann $\deg p = \deg q_1 + \deg q_2$ und somit $\deg q_1 = 1$ oder $\deg q_2 = 1$. Also besäße p einen Teiler vom Grad 1; dieser wäre bis auf Normierung ein Linearfaktor, weshalb p ein Nullstelle hätte.

Übung 81.
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 81.
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 82.
Es sei $K(\alpha)/K$ eine endliche, zyklische Körpererweiterung von ungeraden Grad. Zeigen Sie, dass $K(\alpha) = K(\alpha^2)$.

Lösung 82.
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.

Übung 83.
Es sei K ein algebraisch abgeschlossener Körper und L/K eine algebraische Körpererweiterung. Zeigen Sie, dass bereits $L = K$ gilt.

Lösung 83.
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 $a_1, \ldots, a_n \in K$ 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 84.
Zeigen Sie, dass endliche Körpererweiterungen algebraisch sind.

Lösung 84.
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 $a_n, \ldots, a_0 \in K$ mit $a_n \neq 0$. Für das Polynom

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

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

Übung 85.
Es seien $M/L/K$ Körpererweiterungen, so dass M/L und L/K algebraisch sind. Zeigen Sie, dass auch M/K algebraisch ist.

Übung 86.
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 von den beiden Zahlen $\pi + e$ und πe mindestens eine transzendent sein. Es ist nicht bekannt, welches von ihnen es ist.

Lösung 86.
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 87.
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 87.
Für alle $\alpha \in K$ ist $K(\alpha) = K$. Ist $\alpha \in L$ mit $\alpha \notin K$, so ist $K(\alpha)/K$ eine echte Körperweiterung, 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 88.
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 88.
Wir können o.B.d.A. davon ausgehen, dass P normiert ist. Es sei $\alpha \in L$ eine Nullstelle von P. 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 89.
Es sei K ein Körper und $f \in K[T]$ ein irreduzibles Polynom.

1. Zeigen Sie, dass f im Fall $\operatorname{char} K = 0$ separabel ist.
2. Zeigen Sie durch Angabe eines Beispiels, dass f im Fall $\operatorname{char} K > 0$ nicht notwendigerweise separabel ist.

1. Wegen der Irreduziblität von f gilt $\deg f \geq 1$. Wegen $\operatorname{char} K = 0$ folgt, dass $f' \neq 0$. Da aber $\deg f' = \deg f - 1 < \deg f$ gilt, folgt aus der Irreduziblität von f, dass f und f' teilerfremd sind. Also ist f separabel.
2. Ist $p \coloneqq \operatorname{char} K > 0$, so ist das Polynom $f(X) \coloneqq X^p - t \in \mathbb{F}_p(t)[X]$ nach Eisenstein irreduzibel. Es gilt aber $f' = 0$, weshalb f und f' nicht teilerfremd, und f somit nicht separabel ist.

Übung 90.
Zeigen Sie, dass eine Körpererweiterung L/K genau dann algebraisch ist, wenn jeder Zwischenring $K \subseteq R \subseteq L$ bereits ein Körper ist.

Lösung 90.
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.