Übungen zu Einführung in die Algebra

Jendrik Stelzner

17. Februar 2017

Inhaltsverzeichnis

1 Ringtheorie

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

1. Jeder Körper ist faktoriell.

2. Ist K ein Körper, so ist $K[\![X]\!]$ faktoriell.

3. Die Potenzreihe $6X^4 + 5X^3 + 4X^2 + 3X + 2 \in \mathbb{Z}[\![X]\!]$ ist irreduzibel.

4. 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 $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

5. Für alle Ringe R_1 und R_2 gilt $(R_1 \times R_2)[X] \cong R_1[X] \times R_2[X]$.

6. Jeder faktorielle Ring ist unendlich.

7. Für jeden kommutativen Ring R gibt es einen Integritätsbereich S, so dass $R \cong S/I$ für ein Ideal $I \subseteq S$.

8. Jeder endliche Integritätsbereich ist ein Hauptidealring.

9. Ist R ein endlicher kommutativer Ring, so ist $R[X, Y]$ noethersch.

10. Ist R ein Hauptidealring, so ist auch $R[X]$ ein Hauptidealring.

11. Ist R ein Integritätsbereich und $p \in R$ prim, so ist p irreduzibel.

12. Sind $n_1, n_2, n_3 \in \mathbb{Z}$ mit $\operatorname{ggT}(n_1, n_2, n_3) = 1$, 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.

13. Ist R ein endlicher kommutativer Ring mit $p := \operatorname{char} R > 0$ prim, so ist die Abbildung $R \to R$, $x \mapsto x^p$ ein Ringautomorphismus.

Lösung 1.

1. Die Aussage ist wahr: Ein Körper ist ein Hauptidealring, und somit faktoriell (Körper sind sogar schon euklidsch). Die Aussage lässt sich auch konkret zeigen: Ist K ein Körper, so gibt es keine Primelement in K, die leere Menge $\emptyset =: \mathcal{P} \subseteq K$ ist also ein Repräsentantensystem der Primeleme von K. Jedes Element $x \in K$ mit $x \neq 0$ lässt sich nun eindeutig als $x = x \cdot \prod_{p \in \mathcal{P}} p$ darstellen, denn es gilt $x \in K^\times$ und $\prod_{p \in \mathcal{P}} = 1$ ist das leere Produkt.

2. Die Aussage ist wahr: Der Ring $K[\![X]\!]$ ist euklidisch und somit ein Hauptidealring.

3. Die Aussage ist wahr: Wir bezeichnen die gegebene Potenreihe mit f. Sind $g, h \in \mathbb{Z}[\![X]\!]$ mit $g = \sum_{i=0}^{\infty} g_i X^i$, $h = \sum_{i=0}^{\infty} h_i X^i$ und $f = gh$, so ist inbesondere $2 = g_0 h_0$. Aus der Irreduziblität von $2 \in \mathbb{Z}$ folgt, dass $g_0 = \pm 1$ oder $h_0 = \pm 1$, und somit $g \in \mathbb{Z}[\![X]\!]^\times$ oder $h \in \mathbb{Z}[\![X]\!]^\times$ (siehe Übung 14).

4. Die Aussage ist wahr: Ist $\varphi\colon \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ ein Ringhomomorphismus, so gilt für die Elemente $e_1 \coloneqq \varphi(1,0)$ und $e_2 \coloneqq \varphi(0,1)$, dass $e_1^2 = e_1$ und $e_2^2 = e_2$. Deshalb gilt $e_1, e_2 \in \{0,1\}$. Da außerdem $1 = \varphi(1,1) = \varphi(1,0) + \varphi(0,1) = e_1 + e_2$ gilt, muss entweder $e_1 = 1$ und $e_2 = 0$, oder $e_1 = 0$ und $e_2 = 1$. Im ersten Fall gilt $\varphi = \pi_1$, im zweiten Fall gilt $\varphi = \pi_2$.

   Die Aussage lässt sich auch durch Untersuchen von $\ker\varphi$ zeigen: Es ist $\operatorname{im}\varphi$ ein Unterring von $\mathbb{Z}$, also bereits $\operatorname{im}\varphi = \mathbb{Z}$. Also induziert φ einen Isomorphismus $(\mathbb{Z}\times\mathbb{Z})/\ker\varphi \to \mathbb{Z}$. Deshalb ist $\ker\varphi$ ein Primideal, aber kein maximales Ideal in $\mathbb{Z}\times\mathbb{Z}$. Somit ist $\ker\varphi = \mathbb{Z}\times\mathfrak{p}$ oder $\ker\varphi = \mathfrak{p}\times\mathbb{Z}$ für ein Primideal $\mathfrak{p} \subseteq \mathbb{Z}$ (siehe Übung 33 und Übung 34); wäre dabei $\mathfrak{p}$ maximal, so wäre dies auch $\ker\varphi$ (siehe Übung 33), also kommt nur $\mathfrak{p} = 0$ in Frage. Im Fall $\ker\varphi = 0\times\mathbb{Z}$ gilt $\varphi = \pi_1$ und im Fall $\ker\varphi = \mathbb{Z}\times 0$ gilt $\varphi = \pi_2$.

5. 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 Ringhomorphismus

   $$\varphi\colon (R_1\times R_2)[X] \xrightarrow{\pi_1[X]\times\pi_2[X]} R_1[X]\times R_2[X],$$
   $$\sum_j (a_j, b_j) X^j \mapsto \left(\sum_j a_j X^j, \sum_j b_j X^j\right)$$

   resultieren. Die Bijektivität von φ ergibt sich durch direktes Hinsehen.

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

7. Die Aussage ist wahr: Der Ring $S \coloneqq \mathbb{Z}[T_x \mid x \in R]$ ist ein Integritätsbereich, und der Einsetzhomomorphismus $\varphi\colon S \to R$ mit $\varphi(T_x) = x$ für alle $r \in R$ ist surjektiv, induziert also einen Isomorphismus $\overline{\varphi}\colon S/\ker\varphi \to R$.

8. Die Aussage ist wahr: Jeder endliche Integritätsbereich ist bereits ein Körper.

9. Die Aussage ist wahr: R ist noethersch, und nach iterierter Anwendung des Hilbertschen Basissatzes somit auch $R[X][Y] \cong R[X,Y]$.

10. Die Aussage ist falsch: Ist K ein Körper, so ist zwar $R \coloneqq K[X]$ ein Hauptidealring, aber $R[Y] \cong K[X,Y]$ nicht (siehe Übung 18). Allgemeiner ist $R[X]$ genau dann ein Hauptidealring, wenn R bereits ein Körper ist (siehe Übung 26).

11. 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.

12. Die Aussage ist falsch: Man betrachte etwa $n_1 = n_2 = 2$ und $n_3 = 3$ (dann sind n_1, n_2, n_3 zwar insgesamt teilerfremd, nicht jedoch paarweise, weshalb sich der chinesische Restklassensatz nicht anwenden lässt). Hätte das Gleichungssystem immer ein Lösung, so wäre der Ringhomomorphismus

$$\varphi\colon \mathbb{Z} \to \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3, \quad x \mapsto (\overline{x}, \overline{x}, \overline{x})$$

surjektiv. Dies ist aber nicht der Fall, denn für alle $(a_1, a_2, a_3) \in \operatorname{im} \varphi$ gilt $a_1 = a_2$.

13. Die Aussage ist falsch: Die Abbildung σ ist ein Ringhomomorphismus (siehe Übung 17), aber betrachtet man etwa den Fall $R = \mathbb{F}_p[X]/(X^p)$, so gilt $\sigma(\overline{X}) = \overline{X}^p = \overline{X^p} = 0$ und somit $\ker \sigma = \{x \in R \mid x^p = 0\} \neq 0$. (Besitzt R keine nichttrivialen nilpotenten Elemente, etwa falls R ein Integritätsbereich oder sogar ein Körper ist, so ist σ hingegen ein Automorphismus: Dann gilt $\ker \sigma = 0$, und wegen der Endlichkeit von R ist σ damit schon bijektiv.)

Übung 2. *Größte gemeinsame Teiler*

Bestimmen Sie jeweils einen größten gemeinsamen Teiler und drücken sie diesen als Linearkombination der jeweiligen Elemente aus.

1. a) $54, 24 \in \mathbb{Z}$
   b) $270, 192 \in \mathbb{Z}$
   c) $213, 168 \in \mathbb{Z}$
   d) $45, 63, 105 \in \mathbb{Z}$
   e) $105, 70, 42, 30 \in \mathbb{Z}$
2. a) $t^2 + t - 2, t^2 - 3t + 2 \in \mathbb{Q}[t]$
   b) $t^2 + 3, t^2 - 3t + 2 \in \mathbb{Q}[t]$
   c) $t^4 - t^2 - 2t - 1, t^3 - 1 \in \mathbb{Q}[t]$
   d) $t^3 - t^2 + t - 1, t^3 - 3t^2 + 4t - 2 \in \mathbb{Q}[t]$
   e) $t^3 + t^2 + t + 1, t^2 - 1, t^3 - t^2 + t - 1 \in \mathbb{Q}[t]$

Lösung 2.

1. a) Es gilt $\operatorname{ggT}(54, 24) = 6 = 54 - 2 \cdot 24$.
   b) Es gilt $\operatorname{ggT}(270, 192) = 6 = 5 \cdot 270 - 7 \cdot 192$.
   c) Es gilt $\operatorname{ggT}(213, 168) = 3 = 15 \cdot 213 - 19 \cdot 168$.
   d) Es gilt $\operatorname{ggT}(45, 63, 105) = 3 = 36 \cdot 45 - 24 \cdot 63 - 105$.

e) Es gilt $\operatorname{ggT}(105, 70, 42, 30) = 1 = -13 \cdot 15 + 13 \cdot 70 + 13 \cdot 42 - 3 \cdot 30$.

2. Wir wählen die größten gemeinsamer Teiler jeweils so, dass alle auftretenden Polynome ganzzahlig sind.
   a) Es gilt $\operatorname{ggT}(t^2 + t - 2, t^2 - 3t + 2) = 4t - 4 = (t^2 + t - 2) - (t^2 - 3t + 2)$.
   b) Es gilt $\operatorname{ggT}(t^2 + 3, t^2 - 3t + 2) = 28 = (-3t + 10)(t^2 + 3) + (3t - 1)(t^2 - 3t + 2)$.
   c) Es gilt $\operatorname{ggT}(t^4 - t^2 - 2t - 1, t^3 - 1) = t^2 + t + 1 = -t(t^4 - t^2 - 2t + 1) + (t^2 - 1)(t^3 - 1)$.
   d) Es gilt $\operatorname{ggT}(t^3 - t^2 + t - 1, t^3 - 3t^2 + 4t - 2) = 10t - 10$ wobei
   $$10t - 10 = (-6t^2 + 4t)(t^3 - t^2 + t - 1) + (6t^2 + 8t + 10)(t^3 - 3t^2 + 4t - 2).$$
   e) Es gilt $\operatorname{ggT}(t^3 + t^2 + t + 1, t^2 - 1, t^3 - t^2 + t - 1) = 8$ mit
   $$8 = 2(t^3 + t^2 + t + 1) + (t^3 + t^2 + t + 3)(t^2 - 1) - (t^2 + 2t + 3)(t^3 - t^2 + t - 1).$$

Übung 3. *Irreduziblität von Polynomen*
Entscheiden Sie, ob die folgenden Polynome jeweils irreduzibel sind:

1. $f(X) := X^3 - 2 \in \mathbb{Z}[X]$.
2. $f(X) := X^3 + 39X^2 - 4X + 8 \in \mathbb{Z}[X]$.
3. $f(X) := (X - 3)^2 + 1 \in \mathbb{Q}[X]$.
4. $f(X) := 2X^3 - 14X + 2 \in \mathbb{Q}[X]$.
5. $f(X) := 2X^3 - 14X + 2 \in \mathbb{Z}[X]$.
6. $f(X) := X^3 - 18X^2 + 6X + 3 \in \mathbb{Q}[X]$.
7. $f(X) := X^3 - 18X^2 + 6X + 3 \in \mathbb{R}[X]$.
8. $f(X) := X^5 + 15X^2 + 6X + 21 \in \mathbb{Z}[X]$.
9. $f(X) := X^3 + 2X^2 + X + 1 \in \mathbb{Z}[X]$.
10. $f(X) := 2X^4 + 200X^3 + 2000X^2 + 20000X + 20 \in \mathbb{Q}[X]$.
11. $f(X) := X^n - 2t \in K(t)[X]$ für einen Körper K und $n \geq 1$.
12. $f(X, Y) := XY^3 + X^2Y + 5XY^2 + X^2 + 3XY + 2X + Y + 2 \in \mathbb{Q}[X]$.
13. $f(X, Y) := X^3 + Y^3 + X^2Y + XY^2 + XY + 6X + 6Y + 3 \in \mathbb{Q}[X, Y]$.
14. $f(X) := X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Q}[X]$ für $p > 0$ prim.
15. $f(X) := X^n + X^{n-1} + \cdots + X + 1 \in \mathbb{Q}[X]$ für $n \geq 3$ ungerade.
16. $f(X) := X^6 + X^3 + 1 \in \mathbb{Q}[X]$.

Lösung 3.

1. Nach Eisenstein mit dem Primelement $2 \in \mathbb{Z}$ ist das Polynom irreduzibel.

2. Reduzieren bezüglich $3 \in \mathbb{Z}$ liefert das Polynom $\tilde{f}(X) = X^3 + 2X + 2 \in \mathbb{F}_3[X]$. Das Polynom $\tilde{f}$ hat keine Nullstellen, und da es kubisch ist somit irreduzibel. Also ist auch f bereits irreduzibel.

3. 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 $p = 2$.

4. 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.

5. 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.

6. 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.

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

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

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

10. 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.

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

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

13. 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.

14. 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.

15. 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 $f(X)$.

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

17. Es gilt $f(X + 1) = X^6 + 6X^5 + 15X^4 + 21X^3 + 18X^2 + 9X + 3$. Nach Eisenstein mit dem Primelement $3 \in \mathbb{Z}$ ist $f(X + 1)$ irreduzibel, und somit auch $f(X)$.

Übung 4.

Bestimmen Sie, welche der folgenden Ringe isomorph zueinander sind, und welche nicht:

$$\begin{gathered}\mathbb{Z}/25, \quad \mathbb{F}_{25}, \quad \mathbb{F}_5 \times \mathbb{F}_5, \quad \mathbb{F}_5[X]/(X^2), \\ \mathbb{F}_5[X]/(X^2+2), \quad \mathbb{F}_5[X]/(X^2+4), \quad \mathbb{Z}[X]/(5X).\end{gathered}$$

Lösung 4.
Wir bezeichnen die Ring in der gegebenen Reihenfolge mit $R_1, \dots, R_7$. Wir zeigen, dass die Isomorphieklassen der gegebenen Moduln durch $\{R_1\}, \{R_2, R_5\}, \{R_3, R_6\}, \{R_4\}, \{R_7\}$ gegeben sind.

Das Polynom $X^2 + 2 \in \mathbb{F}_5[X]$ hat keine Nullstellen und ist deshalb irreduzibel (da quadratisch). Folglich ist R_4 eine quadratische Körpererweiterung von $\mathbb{F}_5$, also $R_5 \cong \mathbb{F}_{25} = R_2$.

Das Polynom $X^2 + 4 \in \mathbb{F}_5[X]$ zerfällt in $X^2 + 4 = X^2 - 1 = (X-1)(X+1)$. Nach dem chinesischen Restklassensatz gilt daher

$$R_6 = \mathbb{F}_5[X]/((X-1)(X+1)) \cong \mathbb{F}_5[X]/(X-1) \times \mathbb{F}_5[X]/(X+1) \cong \mathbb{F}_5 \times \mathbb{F}_5 = R_3.$$

Es bleibt zu zeigen, dass die Ring R_1, R_2, R_3, R_4, R_7 paarweise nicht isomorph sind.

Während $R_1, \dots, R_6$ endlich sind (mit je 25 Elementen) ist R_7 unendlich, denn nach dem dritten Isomorphiesatz gilt für das Ideal $(X)/(5X) \subseteq \mathbb{Z}[X]/(5X)$, dass

$$(\mathbb{Z}[X]/(5X))/((X)/(5X)) \cong \mathbb{Z}[X]/(X) \cong \mathbb{Z}.$$

Somit ist R_7 zu keinem der anderen Ringe isomorph.

Es bleibt zu zeigen, dass R_1, R_2, R_3, R_4 paarweisen nicht isomorph sind. Da $0 \neq \overline{5} \in R_1$ und $0 \neq \overline{X} \in R_4$ nilpotent sind, aber R_2 und R_3 außer 0 keine nilpotenten Elemete enthalten, gelten $R_1, R_4 \ncong R_2, R_3$.

Es bleibt zu zeigen, dass $R_1 \ncong R_4$ und $R_2 \ncong R_3$. Dass $R_2 \ncong R_3$ folgt daraus, dass R_2 ein Körper ist, R_3 aber nicht. Es gilt $R_4 \cong \mathbb{F}_5^2$ als $\mathbb{F}_5$-Vektorraum; die unterliegende abelsche Gruppe von R_4 ist deshalb $\mathbb{Z}/5 \oplus \mathbb{Z}/5$, die unterliegende abelsche Gruppe von R_1 ist aber $\mathbb{Z}/25$ (und die beiden Gruppen sind nicht isomorph). Also gilt auch $R_1 \ncong R_4$.

Übung 5. *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 5.

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

2. Es gibt einen eindeutigen Ringhomomorphismus $\phi\colon \mathbb{Z} \to Z$ sowie einen eindeutigen Ringhomomorphismus $\psi\colon Z \to \mathbb{Z}$. Es ist auch $\psi \circ \phi\colon \mathbb{Z} \to \mathbb{Z}$ ein Ringhomomorphismus. Die Identität $\mathrm{id}_{\mathbb{Z}}\colon \mathbb{Z} \to \mathbb{Z}$ ist ebenfalls ein 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 6.

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

Lösung 6.

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 7. *Urbilder von Idealen*

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

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

Lösung 7.

1. Es sei $\pi\colon S \to S/\mathfrak{a}$, $s \mapsto \overline{s}$ die kanonische Projektion. Dann ist $\pi\phi$ ein Ringhomomorphismus und somit $\ker(\pi\phi) = \phi^{-1}(\ker \pi) = \phi^{-1}(\mathfrak{a})$ ein Ideal in R.

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

$$\psi\colon R/\mathfrak{q} \to S/\mathfrak{p} \quad \overline{r} \mapsto \overline{\phi(r)}.$$

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

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

Übung 8.

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

$$\begin{aligned} \{\text{Ideale } J \subseteq R \text{ mit } J \supseteq I\} &\longleftrightarrow \{\text{Ideale } K \subseteq R/I\}, \\ J &\longmapsto \pi(J) = J/I, \\ \pi^{-1}(K) &\longleftarrow\!\shortmid K \end{aligned}$$

eine wohldefinierte Bijektion liefert.

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

Lösung 8.

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 7). 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 9.
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 9.

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 8). Der Ring $R/\mathfrak{m}$ ist genau dann ein Körper, wenn $R/\mathfrak{m}$ genau zwei Ideale enthält (siehe Übung 95); 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 10.
Es sei R ein kommutativer Ring und es gebe $n > 1$, so dass $x^n = x$ für jedes $x \in R$ gilt. Zeigen Sie, dass jedes Primideal in R bereits maximal ist.

Lösung 10.
Ist $\mathfrak{p} \subseteq R$ ein Primideal, so gilt $y^n = y$ für jedes $y \in R/\mathfrak{p}$. Ist $y \neq 0$, so lässt sich diese Gleichung durch y teilen, da $R/\mathfrak{p}$ ein Integritätsbereich ist. Deshalb gilt für jedes $y \in R$ bereits $y^{n-1} = 1$, also $y \cdot y^{n-2} = 1$, weshalb y eine Einheit mit $y^{-1} = y^{n-2}$ ist. Somit ist jedes $y \in R/\mathfrak{p}$ mit $y \neq 0$ eine Einheit, also der Integritätsbereich $R/\mathfrak{p}$ bereits ein Körper, und $\mathfrak{p}$ somit bereits maximal.

Übung 11.

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 11.

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 $(n, q) = (\mathrm{ggT}(n, q))$ gilt, ist dies wiederum äquivalent dazu, dass $\mathrm{ggT}(n, q) = 1$ 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

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

(siehe Übung 8). 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 12.

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 12.

1. Das Radikal $\sqrt{I}$ ist als
$$\sqrt{I} = \{r \in R \mid \text{es gibt } n \in \mathbb{N} \text{ mit } r^n \in I\}$$
definiert. Für alle $x \in I$ gilt $x^1 = x \in I$, weshalb $I \subseteq \sqrt{I}$.
Insbesondere ist somit $0 \in \sqrt{I}$, da $0 \in I$. Für $x, y \in \sqrt{I}$ gibt es $n, m \in \mathbb{N}$ mit $x^n, y^m \in I$. Für alle $k = 0, \dots, n+m$ gilt deshalb $x^k \in I$ oder $y^{n+m-k} \in I$, und somit auch
$$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k} \in I.$$
Deshalb ist auch $x + y \in \sqrt{I}$. Für $r \in R$ und $x \in I$ gibt es $n \in \mathbb{N}$ mit $x^n \in I$, weshalb auch
$$(rx)^n = r^n x^n \in I.$$
Somit ist auch $rx \in \sqrt{I}$.

2. Wir wissen bereits, dass $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$. Für $x \in \sqrt{\sqrt{I}}$ gibt es $n \in \mathbb{N}$ mit $x^n \in \sqrt{I}$, und somit auch noch $m \in \mathbb{N}$ mit $(x^n)^m \in I$. Damit ist $x^{nm} \in I$, weshalb auch $\sqrt{\sqrt{I}} \subseteq \sqrt{I}$.

3. I ist genau dann ein echtes Ideal, wenn $1 \notin I$. Da $1^n = 1$ für alle $n \in \mathbb{N}$ ist genau dann $1 \notin I$, wenn $1 \notin \sqrt{I}$. Dies ist wiederum äquivalent dazu, dass $\sqrt{I}$ ein echtes Ideal ist.

4. 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 13.
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 13.
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 14. *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 14.
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 15. *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 15.

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 16.
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 16.
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 11).
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 17. *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 17.

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 $k = 1, \ldots, p-1$ 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 18.

Es sei K ein Körper.

1. Zeigen Sie, dass $(X, Y) \subseteq K[X, Y]$ kein Hauptideal ist.

2. Zeigen Sie, dass das Ideal $(X_1, X_2, X_3, \ldots) \subseteq K[X_i \mid i = 1, 2, 3, \ldots]$ nicht endlich erzeugt ist.

Lösung 18.

1. Wäre $(X, Y) = (f)$ für eine $f \in K[X, Y]$, so wäre $f \mid X$ und $f \mid Y$, also f ein gemeinsamer Teiler von X und Y (sogar schon ein größter gemeinsamer Teiler, siehe Übung 27). Da X und Y teilerfremd sind, muss f bereits eine Einheit in $K[X, Y]$ sein; dann gilt aber $(X, Y) = (1) = K[X, Y]$, was nicht gilt (denn $K[X, Y]/(X, Y) \cong K$).

2. Es sei $R := K[X_i \mid i = 1, 2, 3, \ldots]$. Wir nehmen an, dass $I := (X_i \mid i \in \mathbb{N})$ endlich erzeugt von $f_1, \ldots, f_t \in I$ erzeugt wird. Man bemerke, dass jedes der Polynome in R nur endlich viele Variablen enthält, und dass I aus all jenen Polynomen besteht, deren konstater Term verschwindet. Es folgt, dass $I = \bigcup_{n \geq 1} (X_1, X_2, \ldots, X_n)$; inbesondere gibt es ein $N \geq 1$ mit $f_1, \ldots, f_t \in (X_1, \ldots, X_N)$. Es gilt also

$$I = (f_1, \ldots, f_t) \subseteq (X_1, \ldots, X_N) \subseteq I$$

   und somit $I = (X_1, \ldots, X_N)$. Damit gilt aber auch

$$\begin{aligned} K \cong R/I &\cong K[X_1, X_2, \ldots, X_N, X_{N+1}, X_{N+2}, \ldots]/(X_1, \ldots, X_N) \\ &\cong K[X_{N+1}, X_{N+2}, \ldots] \cong K[X_1, X_2, X_3, \ldots] = R, \end{aligned}$$

   aber R ist kein Körper.

Übung 19. *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 19.
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 20.
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 20.
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 21.
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 21.

1. Für $k \geq 0$ mit $n^k = 0$ gilt $(1-n)(1+n+\dots+n^{k-1}) = 1-n^k = 1$. Also ist $1-n$ eine Einheit mit $(1-n)^{-1} = \sum_{p=0}^{k-1} n^p = \sum_{p=0}^{\infty} n^p$.

2. Da n nilpotent ist, gilt dies auch für $-n$. Nach dem vorherigen Aufgabenteil ist deshalb $1+n = 1-(-n)$ eine Einheit mit $(1+n)^{-1} = (1-(-n))^{-1} = \sum_{p=0}^{\infty}(-1)^p n^p$.

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

Übung 22. *Ideale in der Lokalisierung*
Es sei R ein kommutativer Ring und $S \subseteq R$ eine multiplikative Teilmenge.

1. Zeigen Sie, dass jedes Ideal $J \subseteq R_S$ von der Form $J = I_S$ für ein Ideal $I \subseteq R$ ist.

2. Zeigen Sie, dass $I_S = (a_i/1 \mid i \in I)$ falls $I = (a_i \mid i \in I)$.

3. Zeigen Sie, dass R_S noethersch ist, wenn R noethersch ist.

4. Zeigen oder widerlegen Sie, dass R_S ein Hauptidealring ist, wenn R ein Hauptidealring ist.

Lösung 22.

1. Es sei $I \coloneqq \{r \in R \mid r/1 \in J\}$. Dies ist ein Ideal in I:

   Es gilt $0 \in I$, da $0/1 \in J$. Für $r_1, r_2 \in I$ gelten $r_1/1, r_2/1 \in J$ und somit auch $(r_1+r_2)/1 = r_1/1 + r_2/1 \in J$, also $r_1+r_2 \in I$. Für $r \in I$ und jedes $r' \in R$ gilt $r/1 \in J$ und somit auch $(r'r)/1 = (r'/1)(r/1) \in J$, also $r'r \in I$. Insgesamt zeigt dies, dass I ein Ideal ist.

Alternativ betrachte man den kanonischen Ringhomomorphismus $i\colon R \to R_S$, $r \mapsto r/1$. Für diesen gilt $I = i^{-1}(J)$, also ist I ein Ideal (siehe Übung 7).

Für jedes $r \in I$ und $s \in S$ gilt $r/1 \in J$ und somit auch $r/s = (1/s)(r/1) \in J$, weshalb $I_S \subseteq J$. Für jedes $r/s \in J$ gilt $r/1 = (s/1)(r/s) \in J$ und somit auch $r \in I$, also $r/s \in I_S$. Deshalb gilt auch $J \subseteq I_S$.

2. Es gilt $a_i \in I$ für alle $i \in I$, also $a_i/1 \in I_S$ für alle $i \in I$ und deshalb $(a_i/1 \mid i \in I) \subseteq I_S$. Ist andererseits $r/s \in I_S$ mit $r \in R$, so gilt $r = \sum_{i \in I} r_i a_i$ mit $r_i = 0$ für fast alle $i \in I$. Dann gilt $r/s = \sum_{i \in I} (r_i/s)(a_i/1) \in (a_i \mid i \in I)$. Also gilt auch $I_S \subseteq (a_i/1 \mid i \in I)$.

3. Ist $J \subseteq R_S$ ein Ideal, so gilt nach dem ersten Aussagenteil $J = I_S$ für ein Ideal $I \subseteq J$. Das Ideal I ist endlich erzeugt, da R noethersch ist, also $I = (a_1, \dots, a_n)$. Nach dem zweiten Aussagenteil gilt deshalb $J = I_S = (a_1/1, \dots, a_n/1)$, weshalb J endlich erzeugt. Es ist also jedes Ideal in R_S endlich erzeugt, also R_S noethersch.

4. Gilt $0 \in S$, so ist $R_S = 0$ kein Hauptidealring. Für $0 \notin S$ ist R_S wieder ein Hauptidealring: Analog zum Beweis des vorherigen Aussagenteils erhalten wir, dass jedes Ideal in R_S ein Hauptideal ist. Es bleibt daher nur zu zeigen, dass R_S ein Integritätsbereich ist. Dies folgt aber daraus, dass R ein Integritätsbereich ist, und dass R_S wegen $0 \notin S$ daher als Unterring des Quotientenkörpers $Q(R)$ realisiert werden kann.

Übung 23.

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.

Lösung 23.

1. Es sei $J \subseteq R/I$ ein Ideal. Dann gibt es ein Ideal $J' \subseteq R$ mit $J' \supseteq I$ und $J = J'/I$ (siehe Übung 8). Das Ideal J' ist endlich erzeugt, da R noethersch ist, also $J' = (a_1, \dots, a_n)$. Damit gilt $J = J/I = (\overline{a_1}, \dots, \overline{a_n})$, weshalb auch J endlich erzeugt ist. Der Ring R/I ist also noethersch, da jedes seiner Ideale endlich erzeugt ist.

2. Analog zum Beweis des ersten Aussagenteiles ergibt sich, dass jedes Ideal in R/I ein Hauptideal ist. Damit R/I ein Integritätsbereich ist, muss allerdings noch zusätzlich gefordert werden, dass I ein Primideal ist. Ist etwa K ein Körper, so ist in $K[X]/(X^2)$ zwar jedes Ideal ein Hauptideal, aber $0 \neq \overline{X} \in K[X]/(X^2)$ ist nilpotent, weshalb $K[X]/(X^2)$ kein Integritätsbereich, und somit auch kein Hauptidealring ist.

Übung 24.

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

Lösung 24.

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 25.

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

Lösung 25.

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 26.

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

Lösung 26.

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 $f = f_0 = a_0 p_0 = a p_0$. 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 27.
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 28.

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

Lösung 29.
Wir nehmen an, dass es nur endlich viele normierte, irreduzible Polynome in $K[X]$ gibt, nämlich $p_1, \dots, p_n \in K[X]$. 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 $i = 1, \dots, n$, und somit $p_i \nmid q$ für alle $i = 1, \dots, n$. Da die p_i ein Repräsentantensystem der Primelemente von $K[X]$ sind, widerspricht dies der Existenz einer Primfaktorzerlegung von q.

Übung 30.
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 30.
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 31.
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 31.

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 32).

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 32.
Zeigen Sie, dass es keinen Ring R gibt, so dass $R[X]$ ein Körper ist.

Lösung 32.
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 33.
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 33.

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 $\ker \pi = (\ker \pi_1) \times \cdots \times (\ker \pi_n) = \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n$. Insbesondere 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 $i = 1, \dots, n$ 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 34.

Es seien $R_1, \dots, R_n$ 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 34.

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

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

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

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

Bemerkung. Übung 33 und Übung 34 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 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 $S' := f(S)$ 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:

$$\begin{tikzcd} & R \times R' \arrow[dl, "j"'] \arrow[dr, "i \times i'"] & \\ (R \times R')_{S \times S'} \arrow[rr, "\varphi"] & & R_S \times R'_{S'} \end{tikzcd}$$

3. Zeigen Sie, dass φ ein Isomorphismus ist.

Lösung 36.

1. Es gelten $1 \in S$ und $1' \in S'$ und somit auch $1_{R \times R'} = (1_R, 1_{R'}) \in S \times S'$.

   Für $(s_1, s'_1), (s_2, s'_2) \in S \times S'$ gelten auch $s_1 s'_1 \in S_1$ und $s_2 s'_2 \in S_2$, und deshalb gilt $(s_1 s'_1, s_2, s'_2) \in S \times S'$.

2. Für $(s, s') \in S \times S'$ gelten $i(s) = s/1 \in R_S^\times$ und $i'(s') = s'/1 \in R_{S'}^\times$ und somit $(i \times i')(s, s') = (s/1, s'/1) \in R_S^\times \times R_{S'}^\times = (R_S \times R_{S'})^\times$. Nach der universellen Eigenschaft der Lokalisierung $(R \times R')_{S \times S'}$ setzt sich $i \times i'$ eindeutig zu einem Ringhomomorphismus $\varphi\colon (R \times R')_{S \times S'} \to R_S \times R'_{S'}$ fort, so dass $\varphi \circ j = i \times i'$, d.h. so dass das gegebene Diagramm kommutiert. Konkret gilt $\varphi((r, r')/(s, s')) = (r/s, r'/s')$ für alle $(r, r')/(s, s') \in (R \times R')_{S \times S'}$.

3. Für jedes $(r/s, r'/s') \in R_S \times R'_{S'}$ gilt $(r/s, r'/s') = \varphi((r, r')/(s, s')) \in \operatorname{im} \varphi$, also ist φ surjektiv. Für $(r, r')/(s, s') \in \ker \varphi$ gilt $0 = \varphi((r, r')/(s, s')) = (r/s, r'/s')$. Es ist also $r/s = 0/1$, es gibt also $t \in S$ mit $tr = 0$. Analog gibt es auch $t' \in S'$ mit $t'r' = 0$. Dann ist $(t, t') \in S \times S'$ mit $(t, t')(r, r') = (tr, t'r') = 0$, weshalb $(r, r')/(s, s') = 0$ gilt. Also ist $\ker \varphi = 0$ und φ somit auch injektiv.

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.
Der Hilbertsche Basissatz besagt, dass für einen noetherschen Ring R auch der Polynomring $R[X]$ noethersch ist.

Zum Beweis des Satzes sei $I \subseteq R[X]$ ein Ideal. Für jedes $d \geq 0$ sei

$$I_d \coloneqq \{a \in R \mid \text{es gibt } f \in I \text{ mit } \deg f = d \text{ und Leitkoeffizienten } a\} \cup \{0\}.$$

Behauptung. Für jedes $d \geq 0$ ist $I_d \subseteq R$ ein Ideal

Beweis. Per Definition gilt $0 \in I_d$. Sind $a_1, a_2 \in I_d$ so gibt es Polynome $f_1, f_2 \in I$ vom Grad d, so dass a_i der Leitkoeffizient von f_i ist. Ist $a_1 = -a_2$, so gilt $a_1 + a_2 \in I_d$; andernfalls löschen sich in der Summe $f_1 + f_2 \in I$ die beiden Leitkoeffizienten nicht aus, weshalb $f_1 + f_2$ ein Polynom von Grad d mit Leitkoeffizienten $a_1 + a_2$ ist. In beiden Fällen gilt $a_1 + a_2 \in I_d$. Ist $r \in R$ und $a \in I_d$, so gibt es ein Polynom $f \in I$ vom Grad d mit Leitkoeffizienten a. Ist $r \cdot a = 0$, so ist insbesondere $r \cdot a \in I_d$; ist $r \cdot a \neq 0$, so ist auch $rf \in I$ wieder vom Grad d und hat ra als Leitkoeffizienten, weshalb auch $ra \in I_d$. □

Ist $f \in I$ vom Grad d mit Leitkoeffizietnen $a \in R$, so ist $Xf \in I$ vom Grad $d + 1$ mit Leitkoeffizienten a. Deshalb ist $I_d \subseteq I_{d+1}$ für alle $d \geq 0$. Da R noethersch ist, stabiliert die aufsteigende Kette $0 \subseteq I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$; es gibt also ein $D \geq 0$ mit $I_D = I_{D+l}$ für alle $l \geq 0$. Die Ideale $I_0, \dots, I_D$ sind endlich erzeugt, da R noethersch sind; Für jedes $d = 0, \dots, D$ sei $I_d = (a_1^{(d)}, \dots, a_{s_d}^{(d)})$. Für jedes $d = 0, \dots, D$ und $i = 1, \dots, s_d$ gibt es dann ein Polynom $f_i^{(d)} \in I$ vom Grad d mit Leitkoeffizienten $a_i^{(d)}$; man merke für $d = 0$, dass $f_i^{(0)} = a_i^{(0)}$ für alle $i = 0, \dots, d$, da ein konstantes Polynom mit seiem Leitkoeffizienten übereinstimmt. Es sei $J \coloneqq (f_i^{(d)} \mid d = 0, \dots, D, i = 1, \dots, s_d) \subseteq I$.

Wir zeigen, dass bereits $J = I$ gilt, dass also $f \in J$ für jedes $f \in I$. Wir zeigen dies per Induktion über den Grad von f: Für $\deg f = 0$ gilt bereits $f \in I_0$, und es gilt

$$I_0 = (a_1^{(0)}, \dots, a_{s_0}^{(0)})_R \subseteq (a_1^{(0)}, \dots, a_{s_0}^{(0)})_{R[X]} = (f_1^{(0)}, \dots, af_{s_0}^{(0)})_{R[X]} \subseteq J.$$

Es sei nun $f \in I$ mit $d \coloneqq \deg f \geq 1$ und es gelte $g \in J$ für alle $f \in I$ mit $\deg g \leq d - 1$. Es sei $a \in I_d$ der Leitkoeffizient von f. Wir unterscheiden zwischen zwei Fällen:

- Gilt $d \leq D$, so gilt $a \in I_d = (a_1^{(d)}, \dots, a_{s_d}^{(d)})$, also $a = \sum_{i=1}^{s_d} r_i a_i^{(d)}$ für passende $r_i \in R$. Das Polynom $g \coloneqq \sum_{i=1}^{s_d} r_i f_i^{(d)} \in J$ hat dann a als Leitkoeffzienten und hat ebenfalls Grad d. Das Polynom $f - g \in I$ hat daher echt kleineren Grad als f, weshalb nach Induktionsvoraussetzung $f - g \in J$ gilt. Somit ist auch $f = (f - g) + g \in J$.

- Gilt $d \geq D$, so ist $a \in I_d = I_D$. Es gilt daher $a = \sum_{i=1}^{s_D} r_i a_i^{(D)}$ für passende $r_i \in R$. Das Polynom $g \coloneqq \sum_{i=1}^{s_D} r_i f_i^{(D)} \in J$ hat dann a als Leitkoeffizienten und Grad $D \leq d$. Deshalb ist $X^{d-D} g \in J$ mit Leitkoeffizienten a und Grad d. Das Polynom $f - X^{d-D} g$ hat daher echt kleineren Grad als f, weshalb nach Induktionsvoraussetzung $f - X^{d-D} g \in J$ gilt. Somit ist auch $f = (f - X^{d-D} g) + X^{d-D} g \in J$.

In beiden Fällen erhalten wir also, dass auch $f \in J$.

Ingesamt zeigt dies, dass $I = J$ endlich erzeugt ist. Der Ring $R[X]$ ist also noethersch, da jedes seiner Ideale endlich erzeugt ist.

Übung 41. *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 42.
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 43.
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 43.

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 44.
Es sei K ein Körper. Zeigen Sie, dass der Ring $K[\![X]\!]$ ein eindeutiges maximales Ideal besitzt.

Lösung 44.
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 $g := \sum_{j=0}^{\infty} f_{n+j} X^j$. 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 $\mathfrak{m} := \{f \in K[\![X]\!] \mid f_0 = 0\}$. 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 45. *Multiple Choice*
Es sei R ein kommutativer Ring. Entscheiden Sie, welche der folgenden Aussagen wahr oder falsch sind.

1. Jeder $\mathbb{Z}/(15, 36)$-Modul trägt eine eindeutige $\mathbb{Z}/(30, 192)$-Modulstruktur.
2. Die abelsche Gruppe $\mathbb{Q}/\mathbb{Z}$ ist endlich erzeugt.
3. Ist K ein Körper, so gilt für alle $a, b \in K$, dass $K[X]/(X - a) \cong K[X]/(X - b)$ als $K[X]$-Moduln.
4. Ist M ein freier R-Modul und $S \subseteq R$ ein Unterring, so ist M auch als S-Modul frei.
5. Ist M ein freier R-Modul endlichen Rangs, so ist auch jeder Untermodul $N \subseteq M$ frei.
6. Ist jeder R-Modul frei, so ist R ein Körper.
7. Ist M ein R-Modul und $N \subseteq M$ ein Untermodul, so gibt es einen Untermodul $P \subseteq M$ mit $M = N \oplus P$.
8. Sind M und N zwei freie R-Moduln endlichen Rangs, so ist auch $\mathrm{Hom}_R(M, N)$ ein freier R-Modul endlichen Rangs.
9. Ist M ein endlich erzeugter R-Modul, so ist auch jeder Untermodul $N \subseteq M$ endlich erzeugt.
10. 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.
11. Ist M ein endlich erzeugter R-Modul und $E \subseteq M$ ein minimales Erzeugendensystem, so ist E endlich.
12. Ist M ein freier R-Modul endlichen Rangs und sind $E_1, E_2 \subseteq M$ zwei minimale Erzeugendensysteme, so sind E_1 und E_2 gleichmächtig.
13. 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.
14. Ist R ein Hauptidealring, so spaltet jede kurze exakte Sequenz von endlich erzeugten torsionsfreien R-Moduln.
15. Ist P ein projektiver R-Modul, so gibt es einen R-Moduln C, so dass $P \oplus C$ frei ist.
16. Sind M_1 und M_2 zwei R-Moduln und $N_1 \subseteq M_1$, $N_2 \subseteq M_2$ Untermoduln mit $M_1 \cong M_2$ und $N_1 \cong N_2$, so gilt auch $M_1/N_1 \cong M_2/N_2$.
17. Ist M ein R-Modul mit $M \cong M \oplus M$, so gilt $M = 0$.

Lösung 45.

1. Die Aussage ist wahr: Es gilt $(15, 36) = (\mathrm{ggT}(15, 36)) = (\mathrm{ggT}(3 \cdot 5, 2^2 \cdot 3^2)) = (3)$ sowie analog $(30, 192) = (\mathrm{ggT}(30, 192)) = (\mathrm{ggT}(2 \cdot 3 \cdot 5, 2^6 \cdot 3)) = (2 \cdot 3) = (6)$. Also gilt $\mathbb{Z}/(15, 36) = \mathbb{Z}/3$ und $\mathbb{Z}/(30, 192) = \mathbb{Z}/6$.

   Eine $\mathbb{Z}/n$-Modulstruktur auf einer abelschen Gruppe A entspricht einer $\mathbb{Z}$-Modulstruktur auf A, so dass $n \cdot A = 0$ (siehe Übung 52). Jede abelsche Gruppe trägt eine eindeutige $\mathbb{Z}$-Modulstruktur (siehe Übung 48), also gilt es nur zu überprüfen, dass aus $3 \cdot A = 0$ bereits $6 \cdot A = 0$ folgt. Dies ist klar, da $3 \mid 6$.

2. Die Aussage ist falsch:

   - Wir haben eine kurze exakte Sequenz von $\mathbb{Z}$-Moduln $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$. Dabei ist $\mathbb{Z}$ endlich erzeugt; wäre $\mathbb{Q}/\mathbb{Z}$ endlich erzeugt, so wäre dies deshalb auch $\mathbb{Q}$ (siehe Übung 60), was aber nicht gilt (siehe Übung 49).

3. Die Aussage ist falsch: Es gibt $a, b \in K$ mit $a \neq b$. Dann sind $K[X]/(X - a)$ und $K[X]/(X - b)$ nicht isomorph als $K[X]$-Moduln:

   - Wegen $a \neq b$ gilt $(X - a) \neq (X - b)$. Nach dem Hauptsatz über endlich erzeugte $K[X]$-Moduln sind die beiden Torsionsmoduln $K[X]/(X - a)$ und $K[X]/(X - b)$ sind also nicht isomorph.
   - Wäre $K[X]/(X - a) \cong K[X]/(X - b)$ als $K[X]$-Moduln, so wäre nach Übung 70 bereits $(X - a) = (X - b)$ und somit $a = b$.
   - Wenn es einen Isomorphismus $\varphi\colon K[X]/(X - a) \to K[X]/(X - b)$ gebe, so würde das folgende Diagramm kommutieren:

   $$\begin{tikzcd} K[X]/(X-a) \arrow[r, "X\cdot"] \arrow[d, "\varphi"] & K[X]/(X-a) \arrow[d, "\varphi"] \\ K[X]/(X-b) \arrow[r, "X\cdot"] & K[X]/(X-b) \end{tikzcd}$$

   Der obere horizontale Pfeil ist durch Multiplikation mit $a \in K$ gegeben, denn für alle $p \in K[X]$ gilt $X \cdot \overline{p} = \overline{Xp} = \overline{ap} = a\overline{p}$. Analog ergibt sich, dass der untere horizontale Pfeile durch Multiplikation mit $b \in K$ gegeben ist. Es müsste also das folgende Diagramm kommutieren:

   $$\begin{tikzcd} K[X]/(X-a) \arrow[r, "a\cdot"] \arrow[d, "\varphi"] & K[X]/(X-a) \arrow[d, "\varphi"] \\ K[X]/(X-b) \arrow[r, "b\cdot"] & K[X]/(X-b) \end{tikzcd}$$

   Es müsste also $\varphi(a \cdot f) = b \cdot \varphi(f)$ für alle $f \in K[X]/(X - a)$. Da φ als Homomorphismus von $K[X]$-Moduln insbesondere K-linear ist, gilt aber $\varphi(a \cdot f) = a \cdot \varphi(f)$ für alle $f \in K[X]/(X - a)$. Wählt man nun $f \in K[X]/(X - a)$ mit $f \neq 0$, so wäre auch $\varphi(f) \neq 0$, und wir erhalten aus $a \cdot \varphi(f) = b \cdot \varphi(f)$, dass $a = b$.

4. 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.

5. Die Aussage ist falsch: Man betrachte für eine Körper K den Ring $R = K[X, Y]$. Dann ist $M = R$ frei vom Rang 1. Der Untermodul, d.h. das Ideal $(X, Y) \subseteq R$ ist aber nicht frei: Da (X, Y) kein Hauptideal ist (siehe Übung 18) müsste (X, Y) frei vom Rang ≥ 2 sein. Inbesondere wäre dann $(X, Y) = I \oplus J$ für zwei Ideale $I, J \subseteq R$ mit $I, J \neq 0$. (Man wähle I als den Span eines Basiselements, und J als den Span aller anderen.) Dann gibt es aber $f \in I$ und $g \in J$ mit $f, g \neq 0$. Wegen der Nullteilerfreiheit von R ist dann auch $fg \neq 0$, da aber $fg \in IJ \subseteq I \cap J$ steht dies im Widerspruch zur Direktheit der Summe $I \oplus J$.

6. 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.

7. Die Aussage ist falsch: Es seien etwa $R = \mathbb{Z}$, $M = \mathbb{Z}$ und $N = 2\mathbb{Z}$. Für jeden Untermodul $P \subseteq M$ mit $P \neq 0$ gilt dann $N \cap P \neq 0$; für jeden Untermodul $P \subseteq M$ gilt also $P + N \subsetneq M$ oder $P \cap N \neq 0$.

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

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

als R-Moduln.

9. 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 18). 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.

10. 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.

11. Die Aussage ist wahr: Da F ein endliches Erzeugendensystem besitzt, enthält jedes Erzeugendensystem $E \subseteq M$ bereits ein endliches Erzeugendensystem $E' \subseteq E$ (siehe Übung 54). Ist E bereits minimal, so muss dabei $E = E'$ gelten, und E somit bereits endlich sein.

12. Die Aussage ist falsch: Betrachtet man $R = \mathbb{Z}$ und $M = \mathbb{Z}$, so sind $\{1\}, \{2, 3\} \subseteq \mathbb{Z}$ zwei minimal Erzeugendensysteme, die nicht gleichmächtig sind.

13. Die Aussage ist falsch: Man betrachte für den Ring $R = \mathbb{Z}$ die kurze exakte Sequenz

$$0 \to \mathbb{Z} \xrightarrow{f} \mathbb{Z} \oplus \bigoplus_{n \geq 2} (\mathbb{Z}/2) \xrightarrow{g} \bigoplus_{n \geq 1} (\mathbb{Z}/2) \to 0$$

wobei $f(n) = (2n, 0, 0, 0, \dots)$ und $g(n, a_1, a_2, a_3, \dots) = (\overline{n}, a_1, a_2, a_3, \dots)$. Diese Sequenz spaltet nicht: Ansonsten gebe es nämlich einen Homomorphismus von R-Moduln $s\colon \mathbb{Z} \oplus \bigoplus_{n\geq 1}(\mathbb{Z}/2) \to \mathbb{Z}$ mit $s \circ f = \mathrm{id}_{\mathbb{Z}}$. Dann würde inbesondere

$$2s(1, 0, 0, \dots) = s(2, 0, 0, \dots) = s(f(1)) = 1$$

gelten, was in $\mathbb{Z}$ nicht möglich ist.

14. Die Aussage ist wahr: Da R ein Hauptidealring ist, ist jeder endlich erzeugte, torsionsfreie Modul bereits frei, und somit inbesondere projektiv. Somit endet jede solche kurze exakte Sequenz in einem projektiven Moduln und spaltet daher (siehe Übung 56).

15. Die Aussage ist wahr: Es gibt einen surjektiven Modulhomomorphismus $\varphi\colon F \to P$ für einen freien R-Modul F (siehe Übung 53). Der Homomorphismus φ lässt sich zu einer kurzen exakten Sequenz $0 \to \ker\varphi \xrightarrow{i} F \xrightarrow{\varphi} P \to 0$ ergänzen, wobei $i\colon \ker\varphi \to F$, $x \mapsto x$ die kanonische Inklusion bezeichnet. Da P projektiv ist, spaltet diese Sequenz, weshalb $P \oplus \ker\varphi \cong F$ frei ist. (Man siehe Übung 56 für die verschiedenen Charakterisierungen projektiver Moduln.)

16. Die Aussage ist falsch: Man siehe Übung 75 für ein Gegenbeispiel.

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

Übung 46.

Bestimmen Sie die Smith-Normalform der folgenden Matrizen $A_i \in \mathrm{Mat}(m \times n, R)$ für den jeweils gegebenen euklidischen Ring R. Bestimmen Sie auch jeweils die Isomorphieklasse von $M_i \coloneqq R^m/AR^n$ gemäß des Hauptsatzes über endlich erzeugte R-Moduln, sowie die Primärzerlegung des Torsionsuntermoduls $T(M_i)$.

1. Es sei $R = \mathbb{Z}$, und es seien

$$A_1 = \begin{pmatrix} 38 & -12 \\ 18 & -6 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 10 & 8 \\ -2 & 6 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 8 & 8 & -2 \\ 10 & 2 & 2 \end{pmatrix}, \quad A_4 = \begin{pmatrix} 1 & 2 & 3 \\ -2 & 3 & 1 \\ 3 & 2 & 1 \end{pmatrix},$$

$$A_5 = \begin{pmatrix} 2 & 4 & 6 \\ 4 & 3 & 7 \\ 11 & -2 & 3 \end{pmatrix}, \quad A_6 = \begin{pmatrix} 15 & 11 & 10 \\ 3 & 2 & -2 \\ 15 & 10 & 11 \end{pmatrix}, \quad A_7 = \begin{pmatrix} -1 & 1 & 0 \\ -2 & -2 & 1 \\ 2 & -2 & 0 \\ -1 & -1 & 3 \end{pmatrix}.$$

2. Es sei $R = \mathbb{Q}[t]$, und es seien

$$A_8 = \begin{pmatrix} t^2 & t^4 - t^2 \\ t & t^2 - t \end{pmatrix}.$$

Lösung 46.

1. a) Eine Smith-Normalform ist $A_2' = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 6 \end{smallmatrix}\right)$. Deshalb gilt

$$M_1 \cong \mathbb{Z}/2 \oplus \mathbb{Z}/6 \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/3.$$

Inbesondere ist M_1 ein Torsionsmodul, und es gilt $M_1 = 3M_2 \oplus 2M_2$; dabei ist $3M_2 \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$ der 2-primäre, und $2M_1 \cong \mathbb{Z}/3$ der 3-primäre Anteil von M_2 .

b) Eine Smith-Normalform ist $A_2' = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 38 \end{smallmatrix}\right)$. Deshalb gilt

$$M_2 \cong \mathbb{Z}/2 \oplus \mathbb{Z}/38 \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/19.$$

Inbesondere ist M_2 ein Torsionsmodul, und es gilt $M_2 = 19M_2 \oplus 2M_2$, wobei $19M_2 \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$ der 2-primäre, und $2M_2 \cong \mathbb{Z}/19$ der 19-primäre Anteil von M_2 ist.

c) Eine Smith-Normalform ist $A_3' = \left(\begin{smallmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \end{smallmatrix}\right)$. Deshalb gilt

$$M_3 \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2 \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2.$$

Inbesondere ist M_3 ein 2-primärer Torsionsmodul.

d) Eine Smith-Normalform ist $A_4' = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 28 \end{smallmatrix}\right)$. Deshalb gilt

$$M_4 \cong \mathbb{Z}/28 \cong \mathbb{Z}/4 \oplus \mathbb{Z}/7.$$

Inbesondere ist M_4 ein Torsionsmodul, und es gilt $M_4 = 7M_4 \oplus 4M_4$; dabei ist $7M_4 \cong \mathbb{Z}/2$ der 2-primäre Anteil von M_4 ist, und $4M_4 \cong \mathbb{Z}/7$ der 7-primäre Anteil.

e) Eine Smith-Normalform ist $A_5' = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 60 \end{smallmatrix}\right)$. Deshalb gilt

$$M_5 \cong \mathbb{Z}/60 \cong \mathbb{Z}/4 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/5$$

Inbesondere ist M_5 ein Torsionsmodul und es gilt $M_5 = 15M_5 \oplus 20M_5 \oplus 12M_5$; dabei ist $15M_5 \cong \mathbb{Z}/4$ der 2-primäre Anteil von M_5, und $20M_5 \cong \mathbb{Z}/3$ der 3-primäre Anteil, und $12M_5 \cong \mathbb{Z}/5$ der 5-primäre Anteil.

f) Eine Smith-Normalform ist $A_6' = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 21 \end{smallmatrix}\right)$. Deshalb gilt

$$M_6 \cong \mathbb{Z}/3 \oplus \mathbb{Z}/24 \cong \mathbb{Z}/3 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/7.$$

Inbesondere ist M_6 ein Torsionsmodul, und es gilt $M_6 = 7M_6 \oplus 4M_6$; dabei ist $7M_6 \cong \mathbb{Z}/3 \oplus \mathbb{Z}/3$ der 5-primäre Anteil von M_6 ist, und $3M_6 \cong \mathbb{Z}/7$ der 7-primäre Anteil.

g) Eine Smith-Normalform ist $A_7' = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 10 \\ 0 & 0 & 0 \end{smallmatrix}\right)$. Deshalb gilt

$$M_7 \cong \mathbb{Z} \oplus \mathbb{Z}/10 \cong \mathbb{Z} \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/5.$$

Inbesondere gilt $T(M_7) = 5T(M_7) \oplus 2T(M_7)$, wobei $5T(M_7) \cong \mathbb{Z}/2$ der 2-primäre Anteil von $T(M_7)$ ist, und $2T(M_7) \cong \mathbb{Z}/5$ der 5-primäre Anteil von $T(M_7)$.

2. a) Eine Smith-Normalform ist $A_8' = \left(\begin{smallmatrix} t & 0 \\ 0 & t^4-t^3 \end{smallmatrix}\right)$. Deshalb gilt

$$M_8 \cong \mathbb{Q}[t]/(t) \oplus \mathbb{Q}[t]/(t^4 - t^3) \cong \mathbb{Q}[t]/(t) \oplus \mathbb{Q}[t]/(t^3) \oplus \mathbb{Q}[t]/(t-1).$$

Inbesondere ist M_8 ein Torsionsmodul, und es gilt $M_8 = (t-1)M_8 \oplus t^3 M_8$, wobei $(t-1)M_8 \cong \mathbb{Q}[t]/(t) \oplus \mathbb{Q}[t]/(t^3)$ der t-primäre Anteil von M_8 ist, und $t^3 M_8 \cong \mathbb{Q}[t]/(t-1)$ der $(t-1)$-primäre Anteil.

Übung 47.

Es seien $n, m \geq 1$. Zeigen Sie, dass $\mathbb{Z}/n \oplus \mathbb{Z}/m \cong \mathbb{Z}/\operatorname{ggT}(n,m) \oplus \mathbb{Z}/\operatorname{kgV}(n,m)$.

Lösung 47.

Es sei $\mathcal{P} = \{2, 3, 5, 7, 11, \dots\}$ die Menge der (positiven) Primzahlen. Wir haben Primfaktorzerlegungen $n = \prod_{p \in \mathcal{P}} p^{\nu_p}$ und $m = \prod_{p \in \mathcal{P}} p^{\mu_p}$ mit $\nu_p, \mu_p \geq 0$ für alle $p \in \mathcal{P}$, sowie $\nu_p = 0$ und $\mu_p = 0$ für fast alle $p \in \mathcal{P}$. Wir erhalten Primfaktorzerlegungen

$$\operatorname{ggT}(n,m) = \prod_{p \in \mathcal{P}} p^{\min(\nu_p, \mu_p)} \quad \text{und} \quad \operatorname{kgV}(n,m) = \prod_{p \in \mathcal{P}} p^{\max(\nu_p, \mu_p)}.$$

Nach dem chinesischen Restklassensatz gelten nun

$$\mathbb{Z}/n \oplus \mathbb{Z}/m \cong \bigoplus_{p \in \mathcal{P}} \mathbb{Z}/p^{\nu_p} \oplus \bigoplus_{p \in \mathcal{P}} \mathbb{Z}/p^{\mu_p} \cong \bigoplus_{p \in \mathcal{P}} (\mathbb{Z}/p^{\nu_p} \oplus \mathbb{Z}/p^{\mu_p})$$

sowie analog

$$\mathbb{Z}/\operatorname{ggT}(n,m) \oplus \mathbb{Z}/\operatorname{kgV}(n,m) \cong \bigoplus_{p \in \mathcal{P}} \left(\mathbb{Z}/p^{\min(\nu_p, \mu_p)} \oplus \mathbb{Z}/p^{\max(\nu_p, \mu_p)} \right).$$

Zum Beweis der Aussage genügt es nun zu zeigen, dass

$$\mathbb{Z}/p^{\nu} \oplus \mathbb{Z}/p^{\mu} \cong \mathbb{Z}/p^{\min(\nu,\mu)} \oplus \mathbb{Z}/p^{\max(\nu,\mu)} \qquad \text{für alle } p \in \mathcal{P} \text{ und } \nu, \mu \geq 0.$$

Dies ist aber klar, da die Paare (ν, μ) und $(\min(\nu,\mu), \max(\nu,\mu))$ bis auf Reihenfolge übereinstimmen.

Übung 48.

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

Lösung 48.

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

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

bekannt. Dabei ist

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

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

Übung 49.
Zeigen Sie, dass $\mathbb{Q}$ als abelsche Gruppe nicht endlich erzeugt ist.

Lösung 49.
Wir geben zwei Beweise an:

- Wir nehmen an, dass $\mathbb{Q}$ endlich erzeugt wäre. Dann gebe es $p_1/q_1, \dots, p_n/q_n \in \mathbb{Q}$ mit $\mathbb{Q} = \langle p_1/q_1, \dots, p_n/q_n \rangle_{\mathbb{Z}}$. Dann würde aber

$$\mathbb{Q} = \left\langle \frac{p_1}{q_1}, \dots, \frac{p_n}{q_n} \right\rangle_{\mathbb{Z}} \subseteq \left\langle \frac{1}{q_1 \cdots q_n} \right\rangle_{\mathbb{Z}} \subseteq \mathbb{Q}$$

  gelten, und somit bereits $\mathbb{Q} = \langle 1/(q_1 \cdots q_n) \rangle_{\mathbb{Z}}$. Dies kann nicht sein, da $1/(2q_1 \cdots q_n)$ in diesem $\mathbb{Z}$-Untermodul nicht enhalten ist.

- Da $\mathbb{Z}$ ein als Hauptidealring insbesondere noethersch ist, wäre $\mathbb{Q}$ als endlich erzeugter $\mathbb{Z}$-Modul bereits noethersch (siehe Übung 62). Dann würde jede aufsteigende Kette von $\mathbb{Z}$-Untermoduln stabilisieren (siehe Übung 61). Die Kette

$$\mathbb{Z} \subsetneq \left\langle \frac{1}{2} \right\rangle_{\mathbb{Z}} \subsetneq \left\langle \frac{1}{4} \right\rangle_{\mathbb{Z}} \subsetneq \left\langle \frac{1}{8} \right\rangle_{\mathbb{Z}} \subsetneq \cdots \subsetneq \left\langle \frac{1}{2^n} \right\rangle_{\mathbb{Z}} \subsetneq \left\langle \frac{1}{2^{n+1}} \right\rangle_{\mathbb{Z}} \subsetneq \cdots$$

  stabilisiert aber nicht.

Übung 50.
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 50.
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 51.
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 $M = \mathrm{im}\, e \oplus \ker e$ und dass $e(m + m') = m$ für alle $m \in \mathrm{im}\, e$ und $m' \in \ker e$.

Lösung 51.

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 52.

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 52.

Es sei $\operatorname{End}(M) := \{f \colon M \to M \mid f \text{ ist additiv}\}$. Die R-Modulstruktur auf M entspricht dem Ringhomomorphismus $\lambda \colon R \to \operatorname{End}(M)$, $r \mapsto \lambda_r$ 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 $\overline{\lambda} \colon R/I \to \operatorname{End}(M)$. 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:

$$\begin{tikzcd} R \arrow[r, "\lambda"] \arrow[d, "\pi"'] & \operatorname{End}(M) \\ R/I \arrow[ur, "\overline{\lambda}"'] & \end{tikzcd}$$

   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 $\hat{\lambda} \colon R_S \to \operatorname{End}(M)$. 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:

$$\begin{tikzcd} R_S \arrow[dr, "\hat{\lambda}"] & \\ R \arrow[u, "i"] \arrow[r, "\lambda"] & \mathrm{End}(M) \end{tikzcd}$$

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 53.
Es sei R ein Ring

1. Es sei 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.

2. Folgern Sie, dass jeder R-Modul M Quotient eines freien R-Moduls ist, d.h. dass es einen freien R-Modul F gibt, so dass $M \cong F/K$ für einen geeigneten Untermoduln $K \subseteq F$.

Lösung 53.

1. 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 $\varphi(x) := \sum_{i \in I} r_i m_i$ 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.

2. Es sei F ein freier R-Modul mit Basis $(b_m)_{m\in M}$. Es sei $\varphi\colon F \to M$ der eindeutige Homomorphismus von R-Moduln mit $\varphi(b_m) = m$ für alle $m \in M$. Dann ist φ surjektiv und induziert daher einen Isomorphismus $\overline{\varphi}\colon F/\ker\varphi \to M$, $x \mapsto \varphi(x)$.

Übung 54.
Es sei M ein endlich erzeugter R-Modul. Zeigen Sie, dass jedes Erzeugendensystem $S \subseteq M$ ein endliches Erzeugendensystem enthält.

Lösung 54.
Es sei $\{m_1, \dots, m_s\} \subseteq M$ ein endliches Erzeugendensystem. Da S ein Erzeugendensystem ist, lässt sich jedes m_i als $m_i = r_{i,1}s_{i,1} + \dots + r_{i,t_i}s_{i,t_i}$ mit $t_i \geq 0$, $s_{i,1}, \dots, s_{i,t_i} \in S$ und $r_{i,1}, \dots, r_{i,t_i} \in R$ schreiben. Für $S' := \{s_{i,j} \mid i = 1, \dots, s, j = 1, \dots, t_i\}$ gilt dann $m_i \in \langle S \rangle$ für alle $i = 1, \dots, s$ und deshalb

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

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

Übung 55. *Linksexaktheit von* Hom

Es sei R ein Ring und $0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0$ eine kurze exakte Sequenz von R-Moduln. Zeigen Sie, dass für jeden R-Moduln L auch die induzierte Sequenz

$$0 \to \mathrm{Hom}_R(L, N) \xrightarrow{f_*} \mathrm{Hom}_R(L, M) \xrightarrow{g_*} \mathrm{Hom}_R(L, P)$$

exakt ist.

Lösung 55.
Für $\varphi_1, \varphi_2 \in \mathrm{Hom}_R(L, N)$ gilt wegen der Injektivität von f, dass

$$f_*(\varphi_1) = f_*(\varphi_2) \iff f \circ \varphi_1 = f \circ \varphi_2 \iff \varphi_1 = \varphi_2.$$

Also ist auch f_* injektiv. Für alle $\varphi \in \mathrm{Hom}_R(L, N)$ gilt

$$(g_* \circ f_*)(\varphi) = g_*(f_*(\varphi)) = \underbrace{g \circ f}_{=0} \circ \varphi = 0,$$

also gilt $\mathrm{im}\, f_* \subseteq \ker g_*$. (Die obige Rechnung lässt sich durch $g_* \circ f_* = (g \circ f)_* = 0_* = 0$ abkürzen.)

Es sei $\varphi \in \ker g_*$. Um zu zeigen, dass bereits $\varphi \in \mathrm{im}\, f_*$ gilt, konstruieren wir einen Homomorphismus $\psi\colon L \to N$ mit $\varphi = f_*(\psi) = f \circ \psi$.

$$\begin{tikzcd}
 & L \arrow[dl, dotted, bend right, "\psi"'] \arrow[d, "\varphi"] \\
N \arrow[r, bend right, "f"'] & M
\end{tikzcd}$$

Es gilt $0 = g_*(\varphi) = g \circ \varphi$ und somit $\operatorname{im} \varphi \subseteq \ker g = \operatorname{im} f$. Es sei $\tilde{\varphi}\colon L \to \operatorname{im} f$ die entsprechende Einschränkung von $\tilde{\varphi}$; für die Inklusion $i\colon \operatorname{im} f \to M$ gilt also $\varphi = i \circ \tilde{\varphi}$. Wegen der Injektivität von f schränkt sich f zu einem Isomorphismus $\tilde{f}\colon N \to \operatorname{im} f$ ein; es gilt also $f = i \circ \tilde{f}$.

$$\begin{tikzcd}
 & & L \arrow[d, "\varphi"] \arrow[dl, dashed, "\tilde{\varphi}"] \\
N \arrow[r, dashed, "\tilde{f}"'] \arrow[rr, bend right, "f"'] & \operatorname{im} f \arrow[r, dashed, "i"'] & M
\end{tikzcd}$$

Da f ein Isomorphismus ist, können wir nun $\psi := \tilde{f}^{-1} \circ \tilde{\varphi}\colon L \to N$ definieren.

$$\begin{tikzcd}
 & & L \arrow[d, "\varphi"] \arrow[dl, "\tilde{\varphi}"] \arrow[dll, dashed, bend right, "\psi"'] \\
N \arrow[r, "\tilde{f}"'] \arrow[rr, bend right, "f"'] & \operatorname{im} f \arrow[r, "i"'] \arrow[l, dashed, bend right, "\tilde{f}^{-1}"'] & M
\end{tikzcd}$$

Wir erhalten, dass

$$f_*(\psi) = f_*(\tilde{f}^{-1} \circ \tilde{\varphi}) = f \circ \tilde{f}^{-1} \circ \tilde{\varphi} = i \circ \tilde{f} \circ \tilde{f}^{-1} \circ \tilde{\varphi} = i \circ \tilde{\varphi} = \varphi.$$

Also gilt bereits $\varphi \in \operatorname{im} f_*$, und somit $\ker g_* \subseteq \operatorname{im} f_*$.

Übung 56. *Äquivalente Charakterisierungen projektiver Moduln*
Es sei R ein Ring und P ein R-Modul. Zeigen Sie, dass die folgenden Bedingungen äquivalent sind:

1. Für jede kurze exakte Sequenz von R-Moduln $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ ist auch die induzierte Sequenz

$$0 \to \operatorname{Hom}_R(P, L) \xrightarrow{f_*} \operatorname{Hom}_R(P, M) \xrightarrow{g_*} \operatorname{Hom}_R(P, N) \to 0$$

   exakt.

2. Ist $g\colon M \to N$ ein surjektiver Homomorphismus von R-Modul, so liftet jeder Homomorphismus $\varphi\colon P \to N$ über g, d.h. es gibt einen Homomorphismus $\psi\colon P \to M$, so dass das folgende Diagramm kommutiert:

$$\begin{tikzcd}
 & P \arrow[d, "\varphi"] \arrow[dl, dotted, "\psi"'] \\
M \arrow[r, two heads, "g"] & N
\end{tikzcd}$$

3. Jede kurze exakte Sequenz von R-Moduln $0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0$ spaltet.

4. P ist direkter Summand eines freien R-Moduls, d.h. es gibt einen R-Modul C, so dass $P \oplus C$ frei ist.

Erfüllt P eine (und damit alle) dieser Bedingungen, so heißt P *projektiv.*

Lösung 56.

($1 \implies 2$) Die Sequenz $0 \to \ker g \xrightarrow{i} M \xrightarrow{g} P \to 0$ ist kurz exakt, da g surjektiv ist; dabei bezeichnet $i\colon \ker g \to M, m \mapsto m$ die kanonische Inklusion. Nach Annahme ist daher auch die Sequenz

$$0 \to \operatorname{Hom}_R(P, \ker g) \xrightarrow{i_*} \operatorname{Hom}_R(P, M) \xrightarrow{g_*} \operatorname{Hom}_R(P, N) \to 0$$

exakt. Inbesondere ist g_* surjektiv, weshalb es für $\varphi \in \operatorname{Hom}_R(P, N)$ ein $\psi \in \operatorname{Hom}_R(P, M)$ mit $\varphi = g_*(\psi) = g \circ \psi$ gibt.

($2 \implies 1$) Da $\operatorname{Hom}(P, -)$ linksexakt ist (siehe Übung 55) ist die Sequenz

$$0 \to \operatorname{Hom}_R(P, \ker g) \xrightarrow{i_*} \operatorname{Hom}_R(P, M) \xrightarrow{g_*} \operatorname{Hom}_R(P, N)$$

exakt. Es bleibt also nur zu zeigen, dass g_* bereits surjektiv ist, dass es also für jeden Homomorphismus $\varphi\colon P \to N$ einen Homomorphismus $\psi \in P \to N$ mit $\varphi = g_*(\psi) = g \circ \psi$ gibt. Dies gilt nach Annahme.

($2 \implies 3$) Es gilt zu zeigen, dass es einen Homomorphismus $\psi\colon P \to M$ gibt, so dass $g \circ \psi = \mathrm{id}_P$, d.h. so dass das folgende Diagramm kommutiert:

$$\begin{tikzcd}
 & & & P \arrow[dl, dotted, "\psi"'] \arrow[d, "\mathrm{id}_P"] & \\
0 \arrow[r] & N \arrow[r, "f"] & M \arrow[r, "g"] & P \arrow[r] & 0
\end{tikzcd}$$

Ein solches ψ existiert nach Annahme.

($3 \implies 4$) Es gibt einen freien R-Modul F und einen surjektiven Homomorphismus $g\colon F \to P$ (siehe Übung 53). Der Homomorphismus g lässt sich zu einer kurze exakte Sequenz $0 \to \ker g \xrightarrow{i} F \xrightarrow{g} P \to 0$ erweitern, wobei $i\colon \ker g \to F, x \mapsto x$ die kanonische Inklusion bezeichnet. Nach Annahme spaltet diese kurze Sequenz, weshalb $P \oplus \ker g \cong F$ frei ist.

($4 \implies 2$) Wir zeigen die Aussage zunächst für den Fall, dass P bereits frei ist: Dann gibt es eine Basis $(b_i)_{i \in I}$ von P, und wegen der Surjektivität von g gibt es für jedes $i \in I$ ein $m_i \in M$ mit $g(m_i) = \varphi(b_i)$. Es sei dann $\psi\colon P \to M$ der eindeutige Homomorphismus von R-Moduln mit $\psi(b_i) = m_i$ für alle $i \in I$. Für alle $i \in I$ gilt $(g \circ \psi)(b_i) = g(\psi(b_i)) = g(m_i) = \varphi(b_i)$, und somit bereits $g \circ \psi = \varphi$.

Wir zeigen nun die allgemeine Aussage: Nach Annahme gibt es einen R-Modul C, so dass $P \oplus C$ frei ist. Es sei $\pi\colon P \oplus C \to P$, $(x, y) \mapsto x$ die kanonische Projektion und $\tilde{\varphi} \coloneqq \varphi \circ \pi\colon P \oplus C \to N$. Nach Annahme einen Homomorphismus $\tilde{\psi}\colon P \oplus C \to M$ mit

$g \circ \tilde{\psi} = \tilde{\varphi}$.

$$\begin{tikzcd}
& P \oplus C \arrow[d, dashed, "\pi"] \arrow[ddl, dashed, bend right, "\tilde{\psi}"'] \arrow[dd, dashed, bend left=60, "\tilde{\varphi}"] \\
& P \arrow[d, "\varphi"] \\
M \arrow[r, "g"] & N
\end{tikzcd}$$

Es sei $\iota \colon P \to P \oplus C, x \mapsto (x, 0)$ die kanonische Inklusion und $\psi := \tilde{\psi} \circ \iota \colon P \to N$.

$$\begin{tikzcd}
& P \oplus C \arrow[d, "\pi"] \arrow[ddl, bend right, "\tilde{\psi}"'] \arrow[dd, bend left=60, "\tilde{\varphi}"] \\
& P \arrow[d, "\varphi"] \arrow[u, dashed, bend left, "\iota"] \arrow[dl, dashed, "\psi"'] \\
M \arrow[r, "g"] & N
\end{tikzcd}$$

Man bemerke, dass $\pi \circ \iota = \mathrm{id}_P$, und deshalb

$$g \circ \psi = g \circ \tilde{\psi} \circ \iota = \tilde{\varphi} \circ \iota = \varphi \circ \pi \circ \iota = \varphi \circ \mathrm{id}_P = \varphi.$$

Übung 57.

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 57.

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 58.

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 58 auf freie Moduln beliebigen Rangs.

Lösung 58.

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 $i\colon R^{n-1} \to R^n$, $(x_1, \dots, x_{n-1}) \mapsto (x_1, \dots, x_{n-1}, 0)$ und die Projektion $p\colon R^n \to R$, $(x_1, \dots, x_n) \mapsto x_n$ 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 57). 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 59.

Es sei R ein Hauptidealring und M ein endlich erzeugter R-Modul.

1. Zeigen Sie, dass auch jeder Untermodul $N \subseteq M$ endlich erzeugt ist.

2. Es gebe ein Erzeugendensystem $m_1, \dots, m_t \in M$ Entscheiden Sie, ob jeder Untermodul $N \subseteq M$ ein Erzeugendensystem aus $\leq t$ vielen Elementen besitzt.

Lösung 59.

1. Als Hauptidealring ist R insbesondere noethersch. Als endlich erzeugter R-Modul ist M somit ebenfalls noethersch (siehe Übung 62). Deshalb ist der Untermodul $N \subseteq M$ endlich erzeugt.

2. Die Aussage ist wahr: Es sei $\varphi\colon R^t \to M$ der eindeutige Homomorphismus von R-Moduln mit $\varphi(e_i) = m_i$ für alle $i = 1, \dots, t$ (hier bezeichnet $e_1, \dots, e_t \in R^t$ die Standardbasis). Dann ist φ surjektiv, und deshalb $F := \varphi^{-1}(N)$ ein Untermodul von R^t, für den $\varphi(F) = N$ gilt. Der R-Modul R^t ist frei vom Rang t; da R ein Hauptidealring ist, folgt daraus, dass der Untermodul $F \subseteq R^t$ frei vom Rang $s \leq t$ ist (siehe Übung 58). Ist $b_1, \dots, b_s \in F$ eine Basis, so bilden $\varphi(b_1), \dots, \varphi(b_s)$ ein Erzeugendensystem von $\varphi(F) = N$.

Übung 60.

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 60.

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

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

   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 $r_{s+1}, \ldots, r_t \in R$. Es sei $m' := r_{s+1}m_{s+1} + \cdots + r_t m_t \in M$. 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 $r_1, \ldots, r_s \in R$, 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 61. *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
$$N_0 \subseteq N_1 \subseteq N_2 \subseteq N_3 \subseteq N_4 \subseteq \ldots$$
   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 61.

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

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

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

von Untermoduln von M, die nicht stabilisiert.

(3 $\implies$ 2) Es sei

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

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

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

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

Dann ist $\mathcal{S}$ eine nicht-leere ($0 \in \mathcal{S}$) Menge von Untermoduln von M, und besitzt daher nach Annahme ein maximales Element N'. Wäre $N' \subsetneq N$, so gebe es ein $f \in N$ mit $f \notin N'$. Dann wäre aber $N'' := N' + \langle f \rangle_R$ ein endlich erzeugter Untermodul von N, also ein Element von $\mathcal{S}$, mit $N' \subseteq N''$, was der Maximalität von N' widerspricht. Also muss bereits $N = N'$, und N somit endlich erzeugt sein.

Übung 62.

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 $M_1, \dots, M_s$ auch $M_1 \oplus \dots \oplus M_s$ 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 63.

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 57). 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 60).

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 $R^n = R \oplus \dots \oplus R$ wieder noethersch.

4. Ist M ein R-Modul mit endlichen Erzeugendensystem $\{m_1, \dots, m_n\} \subseteq M$, so ist der eindeutige Modulhomomorphismus $\varphi\colon R^n \to M$ mit $\varphi(e_i) = m_i$ für alle $i = 1, \dots, n$ (also $\varphi(x_1, \dots, x_n) = x_1 m_1 + \cdots + x_n m_n$) 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 64.
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 64 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 64.
Da M noethersch ist stabilisiert die Kette

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

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 65.
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 65.
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 66.

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 66.

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 67.
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 67.
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 95). 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 68.
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 12.

Lösung 68.
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 69.
Es sei M ein R-Modul.

1. Zeigen Sie, dass $\operatorname{Ann}(\langle m \rangle_R) = \operatorname{Ann}(m)$ für jedes $m \in M$.
2. Zeigen Sie, dass $\operatorname{Ann}(\sum_{i \in I} M_i) = \bigcap_{i \in I} \operatorname{Ann}(M_i)$ für jede Familie $(M_i)_{i \in I}$ von Untermoduln $M_i \subseteq M$.
3. Folgern Sie, dass $\operatorname{Ann}(\langle m_i \mid i \in I \rangle_R) = \bigcap_{i \in I} \operatorname{Ann}(m_i)$ für jede Familie $(m_i)_{i \in I}$ von Elementen $m_i \in M$, und dass $\operatorname{Ann}(M) = \bigcap_{m \in M} \operatorname{Ann}(m)$.
4. Zeigen Sie, dass $\sum_{i \in I} \operatorname{Ann}(M_i) \subseteq \operatorname{Ann}(\bigcap_{i \in I} M_i)$ 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 69.

1. Aus der Inklusion $\{m\} \subseteq \langle m \rangle_R$ folgt die Inklusion $\operatorname{Ann}(\langle M \rangle_R) \subseteq \operatorname{Ann}(m)$. Ist andererseits $x \in \operatorname{Ann}(m)$, 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 $\operatorname{Ann}(\sum_{i \in I} M_i) \subseteq \operatorname{Ann}(M_j)$, und somit insgesamt die Inklusion $\operatorname{Ann}(\sum_{i \in I} M_i) \subseteq \bigcap_{i \in I} \operatorname{Ann}(M_i)$. Gilt andererseits $x \in \bigcap_{i \in I} \operatorname{Ann}(M_i)$, 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 $x \in \operatorname{Ann}(\sum_{i \in I} M_i)$. Somit gilt auch $\bigcap_{i \in I} \operatorname{Ann}(M_i) \subseteq \operatorname{Ann}(\sum_{i \in I} M_i)$.
3. Es gilt die Gleichungskette

$$\operatorname{Ann}(\langle m_i \mid i \in I \rangle_R) = \operatorname{Ann}\left(\sum_{i \in I} \langle m_i \rangle_R \right) = \bigcap_{i \in I} \operatorname{Ann}(\langle m_i \rangle_R) = \bigcap_{i \in I} \operatorname{Ann}(m_i)$$

und somit insbesondere $\operatorname{Ann}(M) = \operatorname{Ann}(\sum_{m \in M} \langle m \rangle_R) = \bigcap_{m \in M} \operatorname{Ann}(m)$.

4. Es gilt genau dann $\sum_{i \in I} \operatorname{Ann}(M_i) \subseteq \operatorname{Ann}(\bigcap_{i \in I} M_i)$, wenn $\operatorname{Ann}(M_j) \subseteq \operatorname{Ann}(\bigcap_{i \in I} M_i)$ 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 $\operatorname{Ann}(M_1) = \operatorname{Ann}(M_2) = \operatorname{Ann}(R) = 0$. Deshalb gilt $\operatorname{Ann}(M_1) + \operatorname{Ann}(M_2) = 0$. Andererseits gilt $M_1 \cap M_2 = 0$ und somit $\operatorname{Ann}(M_1 \cap M_2) = \operatorname{Ann}(0) = R \neq 0$.

Übung 70.
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 70.
Für jedes Ideal $K \subseteq R$ gilt $\operatorname{Ann}(R/K) = K$ (siehe Übung 67), und somit gilt

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

Übung 71. *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 71.
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 $f_1, \dots, f_n$ 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 $f_1, \dots, f_n$ paarweise teilerfremd sind, sind es auch $f_1, \dots, f_{n-1}$. 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 $n_1, \dots, n_s \geq 0$ und paarweise verschiedene $\lambda_1, \dots, \lambda_s \in K$. Die Polynome $(T - \lambda_1)^{n_1}, \dots, (T - \lambda_s)^{n_s}$ 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 72. *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 72.

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 73.

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

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

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

Lösung 73.

(1 $\Longrightarrow$ 2) Es sei $m \in M$ mit $M = \langle m \rangle_R$. Dann gilt
$$\mathrm{Ann}(M) = \mathrm{Ann}(\langle m \rangle_R) = \mathrm{Ann}(m) = \{r \in R \mid rm = 0\}.$$
Für den surjektive Homomorphismus von R-Moduln
$$\varphi\colon R \to M, \quad r \mapsto rm$$
gilt deshalb $\ker \varphi = \mathrm{Ann}(M)$. Somit induziert φ einen Isomorphismus von R-Moduln
$$\bar{\varphi}\colon R/\,\mathrm{Ann}(M) \to M, \quad [r] \mapsto rm.$$
(2 $\Longrightarrow$ 3) Man setze $I = \mathrm{Ann}(M)$.

(3 $\Longrightarrow$ 1) Ist $\varphi\colon R/I \to M$ ein Isomorphismus, so gilt
$$M = \varphi(R/I) = \varphi(\langle \overline{1} \rangle_R) = \left\langle \varphi(\overline{1}) \right\rangle_R.$$

Übung 74. *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 74.

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 75. *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 75.
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 $N_1 \cong R \not\cong R^2 \cong N_2$.

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 $M_1 \not\cong M_2$.

Übung 76. *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:
$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r, "f"] \arrow[d, "\varphi_N"] & M \arrow[r, "g"] \arrow[d, "\varphi_M"] & P \arrow[r] \arrow[d, "\varphi_P"] & 0 \\
0 \arrow[r] & N' \arrow[r, "f'"] & M' \arrow[r, "g'"] & P' \arrow[r] & 0
\end{tikzcd}$$

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
$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r, "f"] & M \arrow[r, "g"] \arrow[d, equal] & P \arrow[r] & 0 \\
0 \arrow[r] & \operatorname{im} f \arrow[r, "i"] & M \arrow[r, "p"] & P \arrow[r] & 0
\end{tikzcd}$$
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 76 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 77. *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 78. *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 $K^\times$.

2. Ist G ein Gruppe und $(N_i)_{i \in I}$ eine Familie normaler Untergruppen $N_i \subseteq G$, so ist auch $\bigcap_{i \in I} N_i \subseteq G$ normal.

Lösung 78.

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.

2. Die Aussage ist wahr: Für jedes $g \in G$ gilt nach Annahme $gN_ig^{-1} \subseteq N_i$ für alle $i \in I$; somit gilt auch $g\left(\bigcap_{i \in I} N_i\right) g^{-1} \subseteq \bigcap_{i \in I}(gN_ig^{-1}) \subseteq \bigcap_{i \in I} N_i$.

Übung 79.

Zeigen Sie, dass die symmetrische Gruppe S_n von dem Zykel $\rho = (1\,2\,\ldots\,n)$ und der Permutation $\tau = (1\,2)$ erzeugt wird.

Lösung 79.

Für alle $i = 1, \ldots, n$ gilt $\rho^{i-1}(1) = i$ und $\rho^{i-1}(2) = i + 1$, und somit

$$\rho^{i-1}\tau(\rho^{i-1})^{-1} = \rho^{i-1}(1 \quad 2)(\rho^{i-1})^{-1} = (\rho^{i-1}(1) \quad \rho^{i-1}(2)) = (i \quad i+1).$$

Deshalb gilt $(1 \quad 2), (2 \quad 3), \ldots, (n-1 \quad n) \in \langle \rho, \tau \rangle$. Da S_n von diese Elementartranspositionen erzeugt wird, gilt bereits $S_n \subseteq \langle \rho, \tau \rangle \subseteq S_n$, und somit $S_n = \langle \rho, \tau \rangle$.

Übung 80. *Zur Ordnung*

Es sei G eine endliche Gruppe.

1. Es seien $H, K \subseteq G$ zwei Untergruppen, so dass $|H|$ und $|K|$ teilerfremd sind. Zeigen Sie, dass $H \cap K = 1$.

2. Es sei $N \subseteq G$ eine Untergruppe, so dass H die einzige Untergruppe von Ordnung $|N|$ ist. Zeigen Sie, dass N normal in G ist.

3. Es sei $|G|$ prim. Zeigen Sie, dass G zyklisch ist.

4. Es sei $N \subseteq G$ eine normale Untergruppe, so dass $|N|$ und $[G : N]$ teilerfremd sind. Zeigen Sie, dass N die einzige Untergruppe von G von Ordnung $|N|$ ist.

Lösung 80.

1. Der Schnitt $H \cap K$ ist sowohl von H als auch von K eine Untergruppe. Deshalb gilt $|H \cap K| \mid |H|$ und $|H \cap K| \mid |K|$. Da $|H|$ und $|K|$ teilerfremd sind, gilt bereits $|H \cap K| = 1$ und somit $H \cap K = 1$.

2. Für $g \in G$ ist die Abbildung $c_g \colon G \to G, x \mapsto gxg^{-1}$ ein Gruppenautomorphismus (siehe Übung 86) ist somit auch $c_g(H) = gHg^{-1}$ eine Untergruppe von G von Ordnung $|H|$. Aus der Eindeutigkeit von H bezüglich dieser Eigenschaft folgt, dass bereits $gHg^{-1} = H$ gilt. Da dies für jedes $g \in G$ gilt ist H normal.

3. Es sei $g \in G$ mit $g \neq 1$. Dann ist $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ eine Untergruppe von G, weshalb $|\langle g \rangle| \mid G$ gilt. Da $|G|$ prim ist, gilt also entweder $|\langle g \rangle| = 1$ und somit $\langle g \rangle = 1$ oder $|\langle g \rangle| = G$ und somit $\langle g \rangle = G$. Da $1 \neq g \in \langle g \rangle$ gilt, kann der erste Fall ausgeschlossen werden.

4. Es sei $\pi \colon G \to G/N$ die kanonische Projektion und $H \subseteq G$ eine Untergruppe von Ordnung $|N|$. Dann ist $\pi(H) \subseteq G/N$ eine Untergruppe, weshalb $|\pi(H)| \mid |G/N| = [G : N]$ gilt. Außerdem gilt $|H/(H \cap N)| = [H : H \cap N] \mid |H| = |N|$.

   Aus $\ker \pi|_H = H \cap \ker \pi = H \cap N$ erhalten wir, dass $\pi(H) \cong H/\ker \pi|_H \cong H/(H \cap N)$ gilt. Somit erhalten wir, dass $\pi(H)$ sowohl $[G : N]$ als auch $|N|$ teilt. Da $[G : N]$ und $|N|$ teilerfremd sind folgt hieraus, dass $\pi(H) = 1$ gilt. Es gilt also $H \subseteq \ker \pi = N$, und wegen $|H| = |N|$ somit bereits $H = N$.

Übung 81. *Bahnenkombinatorik*

Es sei G eine Gruppe der Ordnung 77 die auf einer 17-elementigen Menge X wirkt. Zeigen Sie, dass die Wirkung mindestens 3 Fixpunkte hat. (Ein Element $x \in X$ ist ein Fixpunkt falls $g.x = x$ für alle $g \in G$.)

Lösung 81.

Ist $B \in X/G$ eine G-Bahn und $x \in X$ mit $B = G.x$, so gilt $|B| = |G.x| = [G : G_x] \mid |G|$. Für die Ordnung von G gilt $|G| = 77 = 7 \cdot 11$, also ist $|B| \in \{1, 7, 11, 77\}$ für jede G-Bahn $B \in X/G$. Dabei gilt genau dann $|B| = 1$, falls $B = G.x$ für einen Fixpunkt $x \in X$ gilt; es gilt also zu zeigen, dass es mindestens drei einelementige G-Bahnen in X gibt.

Nach der Bahnengleichung gilt $17 = |X| = \sum_{B \in X/G} |B|$. Die einzigen Möglichkeiten, die Zahl 17 als Summe der Zahlen 1, 7, 11 und 77 darzustellen, sind

$$17 = 11 + 6 \cdot 1 = 2 \cdot 7 + 3 \cdot 1 = 7 + 10 \cdot 1 = 17 \cdot 1.$$

In jeder der Möglichkeiten kommt der Summand 1 mindestens dreimal vor, wodurch sich die Aussage ergibt.

Übung 82. *Mehr Bahnenkombinatorik*

Es sei $p > 0$ prim und G eine endliche p-Gruppe.

1. Es sei X eine endliche Menge mit $p \nmid |X|$ und G wirke auf X. Zeigen Sie, dass die Wirkung einen Fixpunkt besitzt, d.h. dass es ein $x \in X$ gibt, so dass $g.x = x$ für alle $g \in G$ gilt. (*Hinweis*: Nutzen Sie die Bahnengleichung.)

2. Zeigen Sie für $G \neq 1$, dass auch $\mathrm{Z}(G) \neq 1$. (*Hinweis*: Lassen sich G auf sich selbst durch Konjugation wirken.)

Lösung 82.

1. Es sei $B \in X/G$ eine G-Bahn. Es gilt genau dann $|B| = 1$, wenn $B = \{x\}$ für einen Fixpunkt $x \in X$. Ist $|B| \neq 1$ und $x \in B$, so folgt aus $|B| = G.x = [G : G_x] \mid |G| = p^r$ mit $r \geq 0$, dass bereits $p \mid |B|$ gilt.

   Aus der Bahnengleichung erhalten wir, dass $|X| = \sum_{B \in X/G} |B|$. Aus $p \nmid |X|$ erhalten wir, dass $p \nmid |B|$ für eine G-Bahn $B \in X/G$. Nach den obigen Beobachtungen erhalten wir, dass es einen Fixpunkt gibt.

2. Es sei $X := G$. Die Gruppe G wirkt auf X durch Konjugation, also durch $g.x = gxg^{-1}$ für alle $g \in G$, $x \in X$ Ein Punkt $x \in X$ ist genau dann ein Fixpunkt wenn $gxg^{-1} = x$ für alle $g \in G$, wenn also $x \in \mathrm{Z}(G)$. Wie im vorherigen Aussagenteil erhalten wir damit, dass für $B \in X/G$ mit $B = G.x$ für $x \in X$ genau dann $p \mid |B|$ gilt wenn $x \notin \mathrm{Z}(G)$ (hier bezeichnet X/G die Menge der G-Bahnen in X, also die Menge der Konjugationsklassen in G, und nicht den Quotienten trivialen G/G). Da $|G| = p^r$ mit $r \geq 1$ gilt, erhalten wir aus der Bahnengleichung, dass

$$0 \equiv |G| = \sum_{B \in X/G} |B| \equiv \sum_{\substack{B \in X/G \\ |B|=1}} |B| = |\mathrm{Z}(G)| \mod p.$$

   Deshalb gilt $p \mid |\mathrm{Z}(G)|$. Insbesondere ist $|\mathrm{Z}(G)| \neq 1$ und somit $\mathrm{Z}(G) \neq 1$.

Übung 83.
Es sei K ein Körper.

1. Zeigen Sie, dass

$$\mathrm{B}_2(K) := \left\{ \begin{pmatrix} a_1 & b \\ 0 & a_2 \end{pmatrix} \,\middle|\, a_1, a_2 \in K^\times, b \in K \right\}.$$

   eine Untergruppe von $\mathrm{GL}_2(K)$ ist.

2. Zeigen Sie, dass $\mathrm{B}_2(K)$ nicht normal in $\mathrm{GL}_2(K)$ ist.

3. Zeigen Sie, dass

$$\mathrm{U}_2(K) := \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \,\middle|\, b \in K \right\}.$$

   eine normale Untergruppe von $\mathrm{B}_2(K)$ ist, und dass $\mathrm{B}_2(K)/\mathrm{U}_2(K) \cong K^\times \times K^\times$.

4. Entscheiden Sie, ob $\mathrm{B}_2(K) \cong \mathrm{U}_2(K) \times K^\times \times K^\times$.

Lösung 83.

1. Die Einheitsmatrix liegt in $\mathrm{B}_2(K)$, da $1 \in K^\times$. Es gilt

$$\begin{pmatrix} a_1 & b \\ 0 & a_2 \end{pmatrix} \begin{pmatrix} a_1' & b' \\ 0 & a_2' \end{pmatrix} = \begin{pmatrix} a_1 a_1' & a_1' b + b' a_2 \\ 0 & a_2 a_2' \end{pmatrix} \tag{14}$$

mit $a_1 a_1', a_2 a_2' \in K^\times$ falls $a_1, a_1', a_2, a_2' \in K^\times$; deshalb ist $\mathrm{B}_2(K)$ abgeschlossen unter Multiplikation ist. Für $\left(\begin{smallmatrix} a_1 & b \\ 0 & a_2 \end{smallmatrix}\right) \in \mathrm{B}_2(K)$ gilt auch

$$\begin{pmatrix} a_1 & b \\ 0 & a_2 \end{pmatrix}^{-1} = \frac{1}{a_1 a_2} \begin{pmatrix} a_2 & -b \\ 0 & a_1 \end{pmatrix} \in \mathrm{B}_2(K),$$

also ist $\mathrm{B}_2(K)$ auch unter Inversion abgeschlossen.

2. Es gilt

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \notin \mathrm{B}_2(K).$$

3. Aus (14) ergibt sich, dass die Abbildung

$$\varphi\colon\ \mathrm{B}_2(K) \to K^\times \times K^\times, \qquad \begin{pmatrix} a_1 & b \\ 0 & a_2 \end{pmatrix} \mapsto (a_1, a_2)$$

ein surjektiver Gruppenhomomorphismus ist, und es gilt $\ker \varphi = \mathrm{U}_2(K)$. Folglich ist $\mathrm{U}_2(K)$ normal in $\mathrm{B}_2(K)$ und $\mathrm{B}_2(K)/\,\mathrm{U}_2(K) \cong \operatorname{im} \varphi = K^\times \times K^\times$.

4. Für $K = \mathbb{F}_2$ sind die Gruppen isomorph: Es gilt $\mathbb{F}_2^\times \cong 1$ und somit auch $\mathbb{F}_2^\times \times \mathbb{F}_2^\times \cong 1$ sowie $\mathrm{B}_2(\mathbb{F}_2) = \mathrm{U}_2(\mathbb{F}_2)$. Deshalb gilt

$$\mathrm{B}_2(\mathbb{F}_2) \cong \mathrm{U}_2(\mathbb{F}_2) \cong \mathrm{U}_2(\mathbb{F}_2) \times \mathbb{F}_2^\times \times \mathbb{F}_2^\times.$$

Für $K \neq \mathbb{F}_2$ sind die Gruppen nicht isomorph: Die Gruppe $\mathrm{B}_2(K)$ ist dann nicht abelsch, denn es gibt $a_1, a_2 \in K^\times$ mit $a_1 \neq a_2$ und somit gilt

$$\begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_1 & a_1 \\ 0 & a_2 \end{pmatrix} \neq \begin{pmatrix} a_1 & a_2 \\ 0 & a_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix}.$$

Die Gruppe $\mathrm{U}_2(K)$, und damit auch die Gruppe $\mathrm{U}_2(K) \times K^\times \times K^\times$, ist allerdings abelsch, denn für alle $b_1, b_2 \in K$ gilt

$$\begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b_1 + b_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b_2 + b_1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix}.$$

Übung 84.
Es sei G eine Gruppe.

1. Es seien $H, H_1, H_2 \subseteq G$ Untergruppen mit $H \subseteq H_1 \cup H_2$, Zeigen Sie dass bereits $H \subseteq H_1$ oder $H \subseteq H_2$ gilt.

2. Folgern Sie: Sind $H_1, H_2 \subseteq G$ seien zwei Untergruppen, so ist $H_1 \cup H_2$ genau dann eine Untergruppe ist, wenn $H_1 \subseteq H_2$ oder $H_2 \subseteq H_1$.

3. 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 84.

1. Würde $H \not\subseteq H_2$ und $H \not\subseteq H_1$ gelten, so gebe es $h_1, h_2 \in H$ mit $h_1 \notin H_2$ und $h_2 \in H_1$. Da $h_1, h_2 \in H \subseteq H_1 \cup H_2$ gilt, müsste allerdings $h_1 \in H_1$ und $h_2 \in H_2$ gelten. Für das Produkt $h_1 h_2$ würde dann $h_1 h_2 \in H_1$ gelten, denn sonst wäre $h_2 = h_1^{-1} h_1 h_2 \in H_1$, im Widerspruch zur Wahl von h_1. Analog ergebe sich aber auch, dass $h_1 h_2 \notin H_2$ gilt. Es müsste aber $h_1 h_2 \in H \subseteq H_1 \cup H_2$ gelten, da H ein Untergruppe ist.

2. 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.

   Ist andererseits $H_1 \cup H_2$ eine Untergruppe, so ergibt sich aus den vorherigen Aufgabenteil mit $H = H_1 \cup H_2$ dass bereits $H_1 \cup H_2 \subseteq H_1$ oder $H_1 \cup H_2 \subseteq H_2$ gilt, und somit $H_2 \subseteq H_1$ oder $H_1 \subseteq H_2$.

3. 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 85. *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 85.
Es sei $p \coloneqq [G : H]$. Da p eine Primzahl ist gilt inbesondere $p \neq 1$, weshalb H eine echte Untergruppe von G ist. Ist $K \subsetneq G$ eine echte Untergruppe von G mit $H \subseteq K$, so gilt wegen der Multiplikativität des Index', dass

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

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

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

Übung 86. *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 86.

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 87.
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 87.

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 $gG_y g^{-1} = G_x$.
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 $x \sim z$.

4 Körpertheorie

Übung 88. *Multiple Choice*

1. Ist L/K eine endliche Körpererweiterung mit $[L:K] \neq 1$, so gilt auch $\mathrm{Gal}(L/K) \neq 1$.

2. Es gilt $\sqrt[4]{2} \in \mathbb{Q}(\sqrt[10]{6})$.

3. Sind $M/L/K$ Körpererweiterungen, so dass M/K normal ist, so ist auch M/L normal.

Lösung 88.

1. Die Aussage ist falsch: Man betrachte etwa $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt[3]{2})$. Jeder Automorphismus $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ muss die Nullstellen des Polynoms $f(X) := X^3 - 2 \in \mathbb{Q}[X]$ permutieren. Die Nullstellen von f sind $\sqrt[3]{2}, \zeta\sqrt[3]{2}$, und $\zeta^2\sqrt[3]{2}$, wobei $\zeta \in \mathbb{C}, \zeta \notin \mathbb{R}$ eine primitive dritte Einheitswurzel ist (etwa $\zeta = e^{2\pi i/3}$). Inbesondere gelten $\zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2} \notin \mathbb{R}$. Da $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ gilt, ist deshalb $\sqrt[3]{2}$ die einzige Nullstelle von f in $\mathbb{Q}(\sqrt[3]{2})$; für jedes $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ muss deshalb $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ gelten, und somit bereits $\sigma = \mathrm{id}_{\mathbb{Q}(\sqrt[3]{2})}$.

2. Die Aussage ist falsch: Das Polynoms $f(X) = X^4 - 2 \in \mathbb{Q}[X]$ hat $\sqrt[4]{2}$ als Nullstelle, und das Polynom $g(X) = X^{10} - 6 \in \mathbb{Q}[X]$ hat $\sqrt[10]{6}$ als Nullstelle. Die beiden Polynome f und g sind normiert und nach Eisenstein mit dem Primelement $2 \in \mathbb{Z}$ irreduzibel. Folglich ist f das Minimalpolynom von $\sqrt[4]{2}$ und g das Minimalpolynom von $\sqrt[10]{6}$, und somit $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = \deg f = 4$ und $[\mathbb{Q}(\sqrt[10]{6}) : \mathbb{Q}] = \deg g = 10$. Wäre $\sqrt[4]{2} \in \mathbb{Q}(\sqrt[10]{6})$, so wäre $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]$ ein Teiler von $[\mathbb{Q}(\sqrt[10]{6} : \mathbb{Q})]$; da $4 \nmid 10$ ist dies nicht der Fall.

3. Die Aussage ist wahr: Siehe Übung 110.

Übung 89.
Es sei $\alpha \in \mathbb{C}$ eine Nullstelle des Polynoms $X^3 - 6X^2 + 9X + 3 \in \mathbb{Q}[X]$.

1. Bestimmen Sie eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\alpha)$.

2. Drücken Sie α^5 und $3\alpha^4 - 2\alpha^3 + 1$ in der obigen Basis aus.

3. Zeigen Sie, dass $\alpha + 2 \neq 0$ und drücken Sie $1/(\alpha + 2)$ in der obigen Basis aus.

Lösung 89.

1. Das Polynom $f(X) := X^3 - 6X^2 + 9X + 3 \in \mathbb{Q}[X]$ ist nach Eisenstein bezüglich des Primelements $3 \in \mathbb{Z}$ irreduzibel. Also ist f das Minimalpolynom von α, und somit $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f = 3$. Deshalb ist $(1, \alpha, \alpha^2)$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\alpha)$.

2. Da α eine Nullstelle von f ist, gilt $\alpha^3 = 6\alpha^2 - 9\alpha - 3$. Somit gilt auch $\alpha^5 = 6\alpha^4 - 9\alpha^3 - 3\alpha^2$ und $\alpha^4 = 6\alpha^3 - 9\alpha^2 - 3\alpha$. Durch sukzessives Einsetzen ergibt sich, dass

$$\alpha^5 = 6\alpha^4 - 9\alpha^3 - 3\alpha^2 = 27\alpha^3 - 57\alpha^2 - 18\alpha = 105\alpha^2 - 261\alpha - 81.$$

Alternativ ergibt sich auch durch Polynomdivision, dass

$$\alpha^5 = (\alpha^2 + 6\alpha + 27)(\alpha^3 - 6\alpha^2 + 9\alpha + 3) + 105\alpha^2 - 261\alpha - 81,$$

wobei der erste Summand verschwindet, da $\alpha^3 - 6\alpha^2 + 9\alpha + 3 = 0$ gilt. Durch sukszessives Einsetzen ergibt sich auch, dass

$$3\alpha^4 - 2\alpha^3 + 1 = 16\alpha^3 - 27\alpha^2 - 9\alpha + 1 = 69\alpha^2 - 153\alpha - 47.$$

Alternativ ergibt sich mithilfe von Polynomdivision, dass

$$3\alpha^4 - 2\alpha^3 + 1 = (3\alpha + 16)(\alpha^3 - 6\alpha^2 + 9\alpha + 3) + 69\alpha^2 - 153\alpha - 47,$$

wobei der erste Summand verschwindet, da $\alpha^3 - 6\alpha^2 + 9\alpha + 3 = 0$ gilt.

3. Es gibt mehrere Möglichkeiten um einzusehen, dass $\alpha + 2 \neq 0$.
   - Dann wäre $\alpha = -2$, aber -2 ist keine Nullstelle von f.
   - Dann wäre $\alpha = -2$, weshalb f eine rationale Nullstelle hätte, was im Widerspruch zur Irreduziblität von f steht.
   - Dann wäre $2 \cdot 1 + 1 \cdot \alpha + 0 \cdot \alpha^2 = 0$ eine nicht-triviale Linearkombination der 0, was der linearen Unabhängigkeit von $(1, \alpha, \alpha^2)$ über $\mathbb{Q}$ widerspricht.

   Mithilfe des euklidischen Algorithmus ergibt sich, dass

$$-(\alpha^3 - 6\alpha^2 + \alpha + 3) + (\alpha + 2)(\alpha^2 - 8\alpha + 25) = 47,$$

   und somit, dass

$$\frac{1}{\alpha + 2} = \frac{1}{47}\alpha^2 - \frac{8}{47}\alpha + \frac{25}{47}.$$

Übung 90.
Es sei $L := \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

1. Zeigen Sie, dass $\sqrt{2}, \sqrt{3} \in L$ und folgern Sie, dass $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
2. Bestimmen Sie den Grad der Erweiterung $L/\mathbb{Q}$.
3. Zeigen Sie, dass $L/\mathbb{Q}$ galoisch ist.
4. Bestimmen Sie $\mathrm{Gal}(L/\mathbb{Q})$, und entscheiden Sie, ob $\mathrm{Gal}(L/\mathbb{Q})$ abelsch ist.

Lösung 90.
1. Es gilt $(\sqrt{2} + \sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3}$ und deshalb

$$\sqrt{2} = \frac{1}{2}\left((\sqrt{2} + \sqrt{3})^2 - 9(\sqrt{2} + \sqrt{3})\right) \in L.$$

   Somit gilt auch $\sqrt{3} = (\sqrt{2} + \sqrt{3}) - \sqrt{3} \in L$. Dass $L \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ ist klar, und dass $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq L$ gilt, folgt aus $\mathbb{Q} \subseteq L$ und $\sqrt{2}, \sqrt{3} \in L$.

2. Wir betrachten die Zwischenerweiterung $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq L$.

   Das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$ ist $f(X) = X^2 - 2 \in \mathbb{Q}[X]$, denn f ist normiert, nach Eisenstein irreduzibel, und hat $\sqrt{2}$ ist als Nullstelle. Deshalb gilt $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

   Da $\sqrt{3}$ eine Nullstelle des Polynoms $g(X) = X^2 - 3 \in \mathbb{Q}(\sqrt{2})[X]$ ist, gilt die Abschätzung $[L : \mathbb{Q}(\sqrt{2})] \leq 2$. Wäre $[L : \mathbb{Q}(\sqrt{2})] < 2$, also $[L : \mathbb{Q}(\sqrt{2})] = 1$ und somit $L = \mathbb{Q}(\sqrt{2})$, so gebe es $a, b \in \mathbb{Q}$ mit $\sqrt{3} = a + b\sqrt{2}$ (denn $\{1, \sqrt{2}\}$ ist eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt{2})$, da $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$). Deshalb würde dann

   $$3 = \sqrt{3}^2 = (a + b\sqrt{2})^2 = a^2 + 2b^2 + ab\sqrt{3}$$

   gelten. Es müsste $a \neq 0$ gelten, denn sonst wäre $\sqrt{3/2} = b \in \mathbb{Q}$, und es müsste auch $b \neq 0$ gelten, denn sonst wäre $\sqrt{3} = a \in \mathbb{Q}$. Also wäre bereits $\sqrt{3} = (3 - a^2 - 2b^2)/(ab) \in \mathbb{Q}$, was aber nicht gilt.

   Es muss also auch $[L : \mathbb{Q}(\sqrt{2})] = 2$ gelten, und somit insgesamt

   $$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

3. Es gilt $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, -\sqrt{2}, -\sqrt{3})$, also wird $L/\mathbb{Q}$ von den Nullstellen des Polynoms $f(X) = (X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$ erzeugt. Somit ist L der Zerfällungskörper von f über $\mathbb{Q}$. Da die Nullstellen von f paarweise verschieden sind, ist f separabel. Also ist L als Zerfällungskörper des separablen Polynoms f bereits galoisch.

4. Da $L/\mathbb{Q}$ galoisch ist, wissen wir, dass $|\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 4$. Außerdem muss jedes $\sigma \in \mathrm{Gal}(L : \mathbb{Q})$ die Nullstellen der rationalen Polynome $X^2 - 2, X^2 - 3 \in \mathbb{Q}[X]$ permutieren; es muss also $\sigma(\sqrt{2}) = \pm\sqrt{2}$ und $\sigma(\sqrt{3}) = \pm\sqrt{3}$. Da L von $\sqrt{2}$ und $\sqrt{3}$ erzeugt wird, ist σ durch die beiden Werte $\sigma(\sqrt{2})$ und $\sigma(\sqrt{3})$ auch schon eindeutig bestimmt.

   Zusammen mit $|\mathrm{Gal}(L/\mathbb{Q})| = 4$ erhalten wir hieraus, dass die vier Automorphismen $\sigma_1, \sigma_2, \sigma_3, \sigma_4\colon\ \mathrm{Gal}(L/\mathbb{Q})$ durch

   $$\sigma_1\colon \begin{cases} \sqrt{2} & \mapsto & \sqrt{2}, \\ \sqrt{3} & \mapsto & \sqrt{3}, \end{cases} \qquad \sigma_2\colon \begin{cases} \sqrt{2} & \mapsto & -\sqrt{2}, \\ \sqrt{3} & \mapsto & \sqrt{3}, \end{cases}$$

   $$\sigma_3\colon \begin{cases} \sqrt{2} & \mapsto & \sqrt{2}, \\ \sqrt{3} & \mapsto & -\sqrt{3}, \end{cases} \qquad \sigma_4\colon \begin{cases} \sqrt{2} & \mapsto & -\sqrt{2}, \\ \sqrt{3} & \mapsto & -\sqrt{3}, \end{cases}$$

   gegeben sind. Insbesondere erhalten wir, dass $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$, weshalb $\mathrm{Gal}(L/\mathbb{Q})$ abelsch ist.

Übung 91.
Es sei $L \coloneqq \mathbb{Q}(\sqrt[4]{2}, i)$.

1. Bestimmen Sie den Grad der Erweiterun $L/\mathbb{Q}$.

2. Zeigen Sie, dass $L/\mathbb{Q}$ galoisch ist.

3. Bestimmen Sie Gal$(L/\mathbb{Q})$.

4. Entscheiden Sie, ob Gal$(L/\mathbb{Q})$ abelsch ist.

Übung 92.
Es sei $L := \mathbb{Q}(\sqrt[4]{2}, i)$.

1. Bestimmen Sie den Grad der Erweiterun $L/\mathbb{Q}$.

2. Zeigen Sie, dass $L/\mathbb{Q}$ galoisch ist.

3. Bestimmen Sie Gal$(L/\mathbb{Q})$.

4. Entscheiden Sie, ob Gal$(L/\mathbb{Q})$ abelsch ist.

Lösung 92.

1. Wir betrachten den Zwischenkörper $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq L$.

   Das Polynom $f(X) = X^4 - 2 \in \mathbb{Q}[X]$ hat $\sqrt[4]{2}$ als Nullstelle, ist normiert, und nach Eisenstein mit $2 \in \mathbb{Z}$ irreduzibel. Also ist f das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}$ und somit $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$.

   Da i eine Nullstelle des Polynoms $X^2 + 1 \in \mathbb{Q}(\sqrt[4]{2})[X]$ ist, gilt $[L : \mathbb{Q}(\sqrt[4]{2})] \leq 2$. Wäre $[L : \mathbb{Q}(\sqrt[4]{2})] = 1$, also $L = \mathbb{Q}(\sqrt[4]{2})$, so wäre $i \in \mathbb{Q}(\sqrt[4]{2})$. Dies ist aber nicht der Fall, da $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$. also ist $[L : \mathbb{Q}(\sqrt[4]{2})] = 2$.

   Somit gilt $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$.

2. Wir betrachten erneut das Polynom $f(X) = X^4 - 2 \in \mathbb{Q}[X]$. Die Nullstellen dieses Polynoms sind $\sqrt[4]{2}$, $i\sqrt[4]{2}$, $-\sqrt[4]{2}$ und $-i\sqrt[4]{2}$. Da $i = (i\sqrt[4]{2})/\sqrt[4]{2}$ gilt, folgt, dass

   $$L = \mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}).$$

   Also wird L von den Nullstellen von f erzeugt, ist also ein Zerfällungskörper von f. Da die Nullstellen von f paarweise verschieden sind, ist f separabel. Also ist L Zerfällungskörper eines separablen Polynoms, und somit galoisch.

3. Da $L/\mathbb{Q}$ Galoisch ist gilt $|\text{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 8$. Da $\sigma \in \text{Gal}(L/\mathbb{Q})$ die Nullstellen der beiden Polynome $X^4 - 2, X^2 + 1 \in \mathbb{Q}[X]$ jeweils permutieren muss, gelten $\sigma(\sqrt[4]{2}) \in \{\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}\}$ und $\sigma(i) = \pm 1$. Da L von $\sqrt[4]{2}$ und i erzeugt wird ist σ durch die beiden Werte $\sigma(\sqrt[4]{2})$ und $\sigma(i)$ auch schon eindeutig bestimmt.

   Zusammen mit $|\text{Gal}(L/\mathbb{Q})| = 8$ erhalten wir, dass die Automorphismen $\sigma_{r,s} \in \text{Gal}(L/\mathbb{Q})$

mit $r = 1,2,3,4$ und $s = 1,2$ durch

$$\sigma_{1,1}\colon \begin{cases} \sqrt[4]{2} & \mapsto & \sqrt[4]{2}, \\ i & \mapsto & i, \end{cases} \qquad \sigma_{1,2}\colon \begin{cases} \sqrt[4]{2} & \mapsto & \sqrt[4]{2}, \\ i & \mapsto & -i, \end{cases}$$

$$\sigma_{2,1}\colon \begin{cases} \sqrt[4]{2} & \mapsto & i\sqrt[4]{2}, \\ i & \mapsto & i, \end{cases} \qquad \sigma_{2,2}\colon \begin{cases} \sqrt[4]{2} & \mapsto & i\sqrt[4]{2}, \\ i & \mapsto & -i, \end{cases}$$

$$\sigma_{3,1}\colon \begin{cases} \sqrt[4]{2} & \mapsto & -\sqrt[4]{2}, \\ i & \mapsto & i, \end{cases} \qquad \sigma_{3,2}\colon \begin{cases} \sqrt[4]{2} & \mapsto & -\sqrt[4]{2}, \\ i & \mapsto & -i, \end{cases}$$

$$\sigma_{4,1}\colon \begin{cases} \sqrt[4]{2} & \mapsto & -i\sqrt[4]{2}, \\ i & \mapsto & i, \end{cases} \qquad \sigma_{4,2}\colon \begin{cases} \sqrt[4]{2} & \mapsto & -i\sqrt[4]{2}, \\ i & \mapsto & -i, \end{cases}$$

gegeben sind.

4. Die Gruppe $\mathrm{Gal}(L/\mathbb{Q})$ ist nicht abelsch, denn

$$\left(\sigma_{(2,1)} \circ \sigma_{(1,2)}\right)\left(\sqrt[2]{4}\right) = \sigma_{(2,1)}\left(\sigma_{(1,2)}\left(\sqrt[2]{4}\right)\right) = \sigma_{(2,1)}\left(\sqrt[2]{4}\right) = i\sqrt[2]{4}$$

sowie

$$\left(\sigma_{(1,2)} \circ \sigma_{(2,1)}\right)\left(\sqrt[2]{4}\right) = \sigma_{(1,2)}\left(\sigma_{(2,1)}\left(\sqrt[2]{4}\right)\right) = \sigma_{(1,2)}\left(i\sqrt[2]{4}\right) = -i\sqrt[2]{4}.$$

(Die Gruppe $\mathrm{Gal}(L/\mathbb{Q})$ ist isomorph zu der Diedergruppe D_8, die Symmetriegruppe eines Quadrats)

Übung 93.
Es sei $\sigma \in \mathrm{Gal}(\mathbb{R}/\mathbb{Q})$.

1. Zeigen Sie, dass für alle $x \in \mathbb{R}$ genau dann $x \geq 0$, wenn $\sigma(x) \geq 0$.
2. Folgern Sie, dass σ streng monoton steigend ist.
3. Folgern Sie, dass σ stetig ist.
4. Folgern Sie, dass $\sigma = \mathrm{id}_{\mathbb{R}}$.

Das zeigt, dass $\mathrm{Gal}(\mathbb{R}/\mathbb{Q}) = 1$.

Lösung 93.

1. Eine reelle Zahl ist genau dann nicht-negativ, wenn sie eine Quadratzahl ist; diese Eigenschaft ist invariant unter Körperautomorphismen.
2. Für alle $x, y \in \mathbb{R}$ gilt

$$x \geq y \iff x - y \geq 0 \iff \sigma(x) - \sigma(y) \geq 0 \iff \sigma(x) \geq \sigma(y).$$

Somit ist σ monoton steigend; dass σ bereits *streng* monoton steigend ist ergibt sich aus der Injektivität von σ.

3. Für alle $x, y \in \mathbb{R}$ mit $x < y$ gilt nach dem vorherigen Aussagenteil, dass genau dann $x < z < y$, wenn $\sigma(x) < \sigma(z) < \sigma(y)$; also bildet σ offene Intervalle auf offene Intervalle ab. Da eine jede offene Menge $U \subseteq$ eine Vereinigung offener Intervalle ist, folgt daraus, dass auch $\sigma(U) \subseteq$ offen ist. Wendet man dieses Resultat auf $\sigma^{-1} \in \mathrm{Gal}(\mathbb{R}/\mathbb{Q})$ an, so ergibt sich, dass für jede offene Teilmenge $U \subseteq \mathbb{R}$ auch $\sigma^{-1}(U)$ offen ist.

4. Da $\mathbb{Q} \subseteq \mathbb{R}$ dicht liegt, folgt aus $\sigma|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ und der Stetigkeit von σ, dass bereits $\sigma = \mathrm{id}_{\mathbb{R}}$ gilt.

Übung 94.
Es sei $f(X) := X^3 - 2X^2 - X + 1 \in \mathbb{Q}[X]$ und $\alpha \in \mathbb{C}$ eine Nullstelle von f.

1. Bestimmen Sie den Grad von $\mathbb{Q}(\alpha)/\mathbb{Q}$.
2. Zeigen Sie, dass auch $\alpha(\alpha - 2)$ eine Nullstelle von f ist.
3. Folgern Sie, dass $\mathbb{Q}(\alpha)/\mathbb{Q}$ galoisch ist.
4. Bestimmen Sie $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ bis auf Isomorphie.

Lösung 94.

1. Durch Reduzieren bezüglich des Primelements $2 \in \mathbb{Z}$ erhält man das kubische Polynom $\tilde{f}(X) = X^3 + X + 1 \in \mathbb{F}_2[X]$. Da $\tilde{f}(0) = \tilde{f}(1) = 1$ hat $\tilde{f}$ keine Nullstellen. Da $\tilde{f}$ kubisch ist, ist $\tilde{f}$ somit bereits irreduzibel. Also ist auch f schon irreduzibel. Folglich ist f bereits das Minimalpolynom von α. Somit gilt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f = 3$.

2. Es gilt
$$\begin{aligned} f(\alpha(\alpha-2)) &= \alpha^3(\alpha-2)^3 - 2\alpha^2(\alpha-2)^2 - \alpha(\alpha-2) + 1 \\ &= \alpha^6 - 6\alpha^5 + 10\alpha^4 - 9\alpha^2 + 2\alpha + 1. \end{aligned}$$
Aus $0 = f(\alpha) = \alpha^3 - 2\alpha^2 - \alpha + 1$ erhalten wir, dass $\alpha^3 = 2\alpha^2 + \alpha - 1$. Somit gelten auch $\alpha^4 = 2\alpha^3 + \alpha^2 - \alpha$, $\alpha^5 = 2\alpha^4 + \alpha^3 - \alpha^2$ und $\alpha^6 = 2\alpha^5 + \alpha^4 - \alpha^3$. Einsetzen von $\alpha^6 = 2\alpha^5 + \alpha^4 - \alpha^3$ liefert
$$\alpha^6 - 6\alpha^5 + 10\alpha^4 - 9\alpha^2 + 2\alpha + 1 = -4\alpha^5 + 11\alpha^4 - \alpha^3 - 9\alpha^2 + 2\alpha + 1.$$
Einsetzen von $\alpha^5 = 2\alpha^4 + \alpha^3 - \alpha^2$ liefert
$$-4\alpha^5 + 11\alpha^4 - \alpha^3 - 9\alpha^2 + 2\alpha + 1 = 3\alpha^4 - 5\alpha^3 - 5\alpha^2 + 2\alpha + 1.$$
Einsetzen von $\alpha^4 = 2\alpha^3 + \alpha^2 - \alpha$ liefert schließlich
$$3\alpha^4 - 5\alpha^3 - 5\alpha^2 + 2\alpha + 1 = \alpha^3 - 2\alpha^2 - \alpha + 1 = 0.$$
Ingesamt gilt also $f(\alpha(\alpha-2)) = \cdots = 0$.

3. Da $\operatorname{char}\mathbb{Q} = 0$ ist $f \in \mathbb{Q}[X]$ als irreduzibles Polynom bereits separabel. Inbesondere sind die Nullstellen α und $\alpha(\alpha-2)$ verschieden. Also hat f in $\mathbb{Q}(\alpha)$ zwei verschiedene Nullstellen; da f kubisch ist, zerfällt f deshalb über $\mathbb{Q}(\alpha)$ bereits in Linearfaktoren. Es ist also $\mathbb{Q}(\alpha)$ der Zerfällungskörper des separablen Polynoms f, und die Erweiterung $\mathbb{Q}(\alpha)/\mathbb{Q}$ somit galoisch.

4. Da $\mathbb{Q}(\alpha)/\mathbb{Q}$ galoisch ist, gilt $|\operatorname{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Da $\mathbb{Z}/3$ bis auf Isomorphie die einzige dreielementige Gruppe ist, gilt also $\operatorname{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong \mathbb{Z}/3$.

Übung 95.
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 95.
($1 \implies 2$) 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 96.
Es sei K ein algebraisch abgeschlossener Körper. Zeigen Sie, dass K unendlich ist.

Lösung 96.
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 97.
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 97.

Wäre p reduzibel, so gebe $q_1, q_2 \in K[T]$ mit $p = q_1q_2$ 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 98.

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 98.

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 99.

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

Lösung 99.

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 100.

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

Lösung 100.

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 101.

Zeigen Sie, dass endliche Körpererweiterungen algebraisch sind.

Lösung 101.
Es sei L/K eine endliche Körpererweiterung und $x \in L$. Für den K-Untervektorraum $\langle\{x^n \mid n \in \mathbb{N}\}\rangle_K \subseteq L$ gilt

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

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

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

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

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

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

Übung 102.
Es seien $M/L/K$ Körpererweiterungen, so dass M/L und L/K algebraisch sind. Zeigen Sie, dass auch M/K algebraisch ist.

Übung 103.
Es sei $x \in M$. Da M/L algebraisch ist gibt es ein Polynom $p(T) \in L(T)$ mit $p \neq 0$ und $p(x) = 0$. Es seien $a_0, \dots, a_n \in L$ die Koeffizienten von p. Da L/K algebraisch ist sind $a_0, \dots, a_n$ algebraisch über K. Für $L' \coloneqq K(a_0, \dots, a_n)$ wird die Erweiterung L'/K von endlich vielen algebraischen Elementen erzeugt und ist deshalb endlich. Es gilt bereits $p(T) \in L'(T)$, weshalb x algebraisch über L' ist. Insbesondere ist deshalb $L'(x)/L'$ endlich. Ingesamt gilt also $[K(x) : K] \leq [L'(x) : K] = [L'(x) : L'][L' : K] < \infty$. Die Erweiterung $K(x)/K$ ist also endlich, und damit algebraisch (siehe Übung 101). Inbesondere ist x algebraisch über K.

Übung 104.
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 104.
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 105.
Es sei L/K eine Körpererweiterung, so dass $p := [L : K]$ 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 105.
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 106.
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 106.
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 107.
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 $p := \operatorname{char} K > 0$, so ist das Polynom $f(X) := X^p - t \in \mathbb{F}_p(t)[X]$ nach Eisenstein irreduzibel. Es gilt aber $f' = 0$, weshalb f und f' nicht teilerfremd, und f somit nicht separabel ist.

Übung 108.
Es sei K ein Körper, L/K eine endliche Körpererweiterung und es seien $K \subseteq L_1, L_2 \subseteq L$ zwei Zwischenkörper.

1. Zeigen Sie für alle $\alpha, \beta \in L$, dass $[K(\alpha, \beta) : K(\alpha)] \leq [K(\beta) : K]$ gilt.
2. Es sei $L_1 L_2 \subseteq L$ der kleinste Unterkörper, der L_1 und L_2 enthält. Zeigen Sie, dass $[L_1 L_2 : L_2] \leq [L_1 : K]$.
3. Zeigen Sie, dass $[L_1 L_2 : K] = [L_1 : K][L_2 : K]$ falls $[L_1 : K]$ und $[L_2 : K]$ teilerfremd sind.

Lösung 108.

1. Da L/K endlich ist, gilt dies auch für $[K(\beta) : K]$. Ist $f(X) \in K[X]$ das Minimalpolynom von β, so gilt $[K(\beta) : K] = \deg f$. Dann ist auch $f(X) \in K(\alpha)[X]$ mit $f(\beta) = 0$; für das Minimalpolynom $g(X) \in K(\alpha)[X]$ von β gilt daher $\deg g \leq \deg f$. Dabei gilt $\deg g = [K(\alpha, \beta) : K(\alpha)]$ und die Aussage folgt.
2. Da L/K endlich erzeugt ist, sind es auch L_1/K und L_2/K. Inbesondere sind die beiden Erweiterungen sind endlich erzeugt, also $L_1 = K(\alpha_1, \ldots, \alpha_n)$ und $L_2 = K(\beta_1, \ldots, \beta_m)$. Inbesondere gilt damit auch $L_1 L_2 = K(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$. Aus dem vorherigen Aussagenteil erhalten wir, dass
$$\begin{aligned}
[L_1 : K] &= [K(\alpha_1, \ldots, \alpha_n) : K] \\
&\geq [K(\alpha_1, \ldots, \alpha_n, \beta_1) : K(\beta_1)] \\
&\geq [K(\alpha_1, \ldots, \alpha_n, \beta_1, \beta_2) : K(\beta_1, \beta_2)] \\
&\geq \cdots \\
&\geq [K(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m) : K(\beta_1, \ldots, \beta_m)] = [L_1 L_2 : L_2].
\end{aligned}$$
3. Aus $K \subseteq L_1, L_2 \subseteq L_1 L_2$ folgt wegen der Multiplikativität des Grades, dass $[L_1 : K]$ und $[L_2 : K]$ den Grad $[L_1 L_2 : K]$ teilen. Wegen der Teilerfremdheit folgt, dass auch $[L_1 : K][L_2 : K]$ ein Teiler von $[L_1 L_2 : K]$ ist. Andererseits gilt nach dem vorherigen Aussagenteil, dass
$$[L_1 L_2 : K] = [L_1 L_2 : L_2][L_2 : K] \leq [L_1 : K][L_2 : K].$$
Ingesamt folgt deshalb $[L_1 L_2 : K] = [L_1 : K][L_2 : K]$.

Übung 109. *Quadratische Körpererweiterungen*
Es sei L/K eine Körpererweiterung vom Grad 2. Es gelte zunächst $\operatorname{char} K \neq 2$.

1. Zeigen Sie, dass $L = K(\alpha)$ für ein $\alpha \in L$ mit $\alpha \notin K$ und $\alpha^2 \in K$ gilt. (L entsteht also durch Hinzuadjungieren einer Quadratwurzel.)
2. Folgern Sie, dass L/K galoisch ist.

Es gelte nun $\operatorname{char} K = 2$.

3. Zeigen Sie, dass L nicht notwendigerweise durch Hinzuadjungieren einer Quadratwurzel entsteht.
4. Zeigen Sie, dass L/K nicht notwendigerweise galoisch ist.

Lösung 109.

1. Ist $\alpha \in L$ mit $\alpha \neq K$, so gilt
$$2 = [L : K) \geq [K(\alpha) : K] \geq 2,$$
also $[K(\alpha) : K] = 2$ und somit $L = K(\alpha)$. Ist $f \in K[X]$ das Minimalpolynom von α, so gilt deshalb $\deg f = [K(\alpha : K] = 2$ und $L = K(\alpha) \cong K[X](f)$. Wir können daher o.B.d.A. davon ausgehen, dass $L = K[X]/(f)$ für ein normiertes, irreduzibles quadratisches Polyom $f \in K[X]$ gilt.

   Da $\operatorname{char} K \neq 2$ gilt, können wir
$$f(X) = X^2 + aX + b = \left(X + \frac{a}{2}\right)^2 - \left(\frac{a^2}{4} - b\right)$$
schreiben. Der Automorphismus $K[X] \to K[X], p(X) \mapsto p(X - a/2)$ induziert deshalb einen Isomorphismus $K[X]/(f) \to K[X]/(X^2 - (a^2/4 - b))$. Wir können also auch o.B.d.A. davon ausgehen, dass f von der Form $f(X) = X^2 - c$ ist, wobei $c \in K$ kein Quadrat ist.

   Wir haben nun also $L = K[X]/(X^2 - c)$, wobei $c \in K$ kein Quadrat ist. Nun leistet $\alpha = \overline{X}$ das Gewünschte.

2. Es sei $\alpha \in L$ mit $\alpha \notin K$ und $\alpha^2 \in K$. Dann ist $f(X) := X^2 - \alpha^2 \in K[X]$ das Minimalpolynom, denn es ist normiert, hat α als Nullstelle, und ist irreduzibel (denn es ist quadratisch und hat keine Nullstelle in K). Es gibt nun (mindestens) zwei mögliche Argumentationsweisen:
   - Der Automorphismus $K[X] \to K[X], p(X) \mapsto p(-X)$ induziert einen K-linearen Automorphismus $K[X]/(f) \to K[X]/(f), a + b\overline{X} \mapsto a - b\overline{X}$. Unter dem Isomorphismus $K[X]/(f) \to L = K(\alpha), a + b\overline{X} \mapsto a + b\alpha$ entspricht dies dem K-linearen Automorphismus $\tau \colon L \to L, a + b\alpha \mapsto a - b\alpha$. Es ergibt sich nun (mindestens) zwei Weisen um einzusehen, dass $|\mathrm{Gal}(L/K)| = 2 = [L : K]$ gilt:
     - Jedes $\sigma \in \mathrm{Gal}(L/K)$ muss die Nullstellen von f permutieren, und somit muss $\sigma(\alpha) = \pm\alpha$ gelten. Da $L = K(\alpha)$ gilt, ist deshalb bereits $\sigma = \mathrm{id}$ (falls $\sigma(\alpha) = \alpha$) oder $\sigma = \tau$ (falls $\sigma(\alpha) = -\alpha$). Es gilt also bereits $\mathrm{Gal}(L/K) = \{\mathrm{id}_L, \tau\}$.
     - Es gilt $2 \leq |\mathrm{Gal}(L/K)| \leq [L : K] = 2$.
   - Da $L = K(\alpha) = K(\alpha, -\alpha)$ gilt, ist L ein Zerfällungskörper von f über K. Die beiden Nullstellen von f, α und $-\alpha$, sind verschieden, da $\alpha \neq 0$ (denn $\alpha \notin K$) und $\operatorname{char} K \neq 2$ gelten. Also ist f separabel. Als Zerfällungskörper eines separablen Polynoms ist L/K galoisch.

3. Wir betrachten den Fall, dass K ein endlicher Körper ist. Dann ist der Frobeniushomomorphismus $\sigma\colon K \to K$, $x \mapsto x^2$ ein Automorphismus, also insbesondere surjektiv. Ist $\alpha \in L$ mit $\alpha^2 \in K$, so gibt es deshalb ein $x \in K$ mit $x^2 = \alpha^2$, also $0 = x^2 - \alpha^2 = (x-\alpha)^2$. Somit gilt dann bereits $\alpha = x \in K$.

4. Wir betrachten den Fall $K = \mathbb{F}_2(t)$. Das Polynom $f(X) = X^2 - t \in \mathbb{F}_2(t)[X]$ ist nach Eisenstein bezüglich des Primelements $t \in \mathbb{F}_2[t]$ irreduzibel. Es gilt aber $f' = 0$, weshalb f nicht separabel ist. Für $L := K[X]/(f)$ ist dann $\overline{X} \in L$ nicht separabel, da f das Minimalpolynom von $\overline{X}$ ist. Somit ist L/K auch nicht galoisch.

Übung 110. *Einschränkung und Transitivität von Normalität*
Es seien $M/L/K$ algebraische Körpererweiterungen.

1. Es sei $\overline{K}$ ein algebraischer Abschluss von K. Zeigen Sie, dass $\overline{K}/K$ normal ist.

2. Zeigen Sie, dass M/L normal ist, falls M/K normal ist.

3. Zeigen Sie, dass L/M nicht notwendigerweise normal ist, falls M/K normal ist.

4. Zeigen Sie, dass M/K nicht notwendigerweise normal ist, wenn M/L und L/K normal sind.

Lösung 110.

1. Jedes Polynom $f \in K[X]$ zerfällt über $\overline{K}$ bereits in Linearfaktoren; inbesondere also jedes irreduzibel Polynom, das eine Nullstelle in $\overline{K}$ hat.

2. Nach Annahme gibt es eine Familie $(f_i)_{i \in I}$ von Polynomen $f_i \in K[X]$, so dass M der Zerfällungskörper der f_i über K ist. Dann ist M auch der Zerfällungskörper der f_i über L, und somit M/L normal.

3. Es sei L/K eine algebraische, nicht normale Körpererweiterung, und $\overline{L}$ ein algebraischer Abschluss von L. Dann ist $\overline{L}$ algebraisch abgeschlossen und $\overline{L}/K$ algebraisch, also $\overline{L}$ auch von K ein algebraischer Abschluss. Nach dem ersten Aussagenteil ist somit $\overline{L}/L/K$ ein Gegenbeispiel.

4. Wir betrachten die Körpererweiterungen $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.

   Es gilt $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$, denn das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}$ ist $X^4 - 2$ (die Irreduziblität ergibt sich mit Eisenstein), und es gilt $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2$, denn das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$ ist $X^2 - 2$ (die Irreduziblität ergibt sich ebenfalls mit Eisenstein). Somit gilt $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = 2$.

   Die beiden Erweiterungen $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ sind also beide vom Grad 2; da $\operatorname{char} \mathbb{Q} \neq 2$ gilt, sind sie somit beide galoisch (siehe Übung 109) und damit insbesondere normal. Die Erweiterung $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ ist allerdings nicht normal, denn das Polynom $f(X) := X^4 - 2 \in \mathbb{Q}[X]$ hat zwar eine Nullstelle in $\mathbb{Q}(\sqrt[4]{2})$, zerfällt dort aber nicht in Linearfaktoren, da die beiden Nullstellen $\pm i\sqrt[4]{2}$ nicht in $\mathbb{Q}(\sqrt[4]{2})$ liegen (denn $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$).

Übung 111.
Zeigen Sie, dass eine Körpererweiterung L/K genau dann algebraisch ist, wenn jeder Zwischenring $K \subseteq R \subseteq L$ bereits ein Körper ist.

Lösung 111.
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.