Übungen mit Lösungen zu Einführung in die Algebra

Jendrik Stelzner

Letzte Änderung: 14. März 2018

Inhaltsverzeichnis

1 Gruppentheorie

Übung 1. *Wahr oder Falsch?*

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.
3. Die Gruppe $\mathbb{Z}/11 \times \mathbb{Z}/13$ ist zyklisch.
4. Jede Gruppe der Ordnung 101 ist abelsch.
5. Ist p prim, so ist jede Gruppe der Ordnung p auflösbar.
6. Ist G ein abelsche Gruppe und $H \subseteq G$ eine Untergruppe, so gilt $G \cong H \times (G/H)$.
7. Ist G eine Gruppe und $N \subseteq G$ eine normale Untergruppe, so dass N und G/N abelsch sind, so ist auch G abelsch.
8. Jede unendliche Gruppe G enthält eine echte, nicht-triviale Untergruppe $H \subsetneq G$.
9. Ist p prim, so ist jede Gruppe der Ordnung p^3 abelsch.
10. Die symmetrische Gruppe S_n wird von dem Zykel $\rho = (1\,2\,\ldots\,n)$ zusammen mit der Permutation $\tau = (1\,2)$ erzeugt.
11. Die Gruppen $\mathbb{C}^\times$ und $\mathbb{R} \times S^1$ sind isomorph.
12. Es gibt eine Untergruppe $H \subseteq \mathbb{C}^\times$ mit $\mathbb{R}^\times \cong \mathbb{C}^\times/H$.
13. Für jede endliche abelsche Gruppe A gilt für das Element $s \coloneqq \sum_{a \in A} a$, dass $2s = 0$.
14. Für die Gruppe $\mathrm{GL}_n(\mathbb{F}_p)$ ist die Untergruppe $\mathrm{U}_n(\mathbb{F}_p) \subseteq \mathrm{GL}_n(\mathbb{F}_p)$ der oberen Dreiecksmatrizen mit 1-en auf der Diagonalen eine p-Sylowuntergruppe.
15. Ist G ein Gruppe, so haben gh und hg für alle $g, h \in G$ dieselbe Ordnung.
16. Wird eine Gruppe G von endlich vielen Elementen endlicher Ordnung erzeugt, so ist G endlich.

Übung 2. *Klassifikation zyklischer Gruppen*

Es sei G eine zyklische Gruppe, d.h. es gebe $g \in G$ mit $G = \langle g \rangle$.

1. Zeigen Sie, dass G abelsch ist.
2. Zeigen Sie, dass $G \cong \mathbb{Z}/n$ für eine eindeutiges $n \in \mathbb{Z}$ mit $n \geq 0$.

Übung 3. *Zur Definition von Untergruppen*
Es sei G eine Gruppe und $H \subseteq G$ eine nichtleere Teilmenge.

1. Zeigen Sie, dass H genau dann eine Untergruppe ist, wenn für alle $x, y \in H$ auch $xy^{-1} \in H$ gilt.

2. Für alle $x, y \in H$ gelte $xy \in H$, und H sei zusammen mit der (Einschränkung der) Multiplikation von G ebenfalls eine Gruppe. Zeigen Sie, dass H bereits eine Untergruppe von G ist.

Übung 4. *Untergruppen von endlichen Gruppen*
Es sei G eine endliche Gruppe. Zeigen Sie, dass eine nichtleere Teilmenge $H \subseteq G$ genau dann eine Untergruppe ist, wenn $xy \in H$ für alle $x, y \in H$ gilt.

Übung 5. *Zur Definition von Gruppen*
Es sei G eine nichtleere Menge zusammen mit einer assoziativen binären Verknüpfung $G \times G \to G$, $(g_1, g_2) \mapsto g_1 g_2$. Zeigen Sie, dass die folgenden Bedingungen äquivalent sind:

i) Es handelt sich bei G um eine Gruppe.

ii) Für alle $a, b \in G$ sind die Gleichungen $ax = b$ und $xa = b$ jeweils eindeutig lösbar.

iii) Für alle $a, b \in G$ sind die Gleichungen $ax = b$ und $xa = b$ jeweils lösbar.

Übung 6. *Die Gruppe G^{op}*
Es sei $(G, \cdot)$ eine Gruppe. Die Gruppe $(G^{\mathrm{op}}, *)$ ist definiert als die zugrundeliegende Menge $G^{\mathrm{op}} \coloneqq G$ zusammen mit der binären Verknüpfung

$$g_1 * g_2 \coloneqq g_2 \cdot g_1$$

für alle $g_1, g_2 \in G^{\mathrm{op}}$.

1. Zeigen Sie, dass $(G^{\mathrm{op}}, *)$ tatsächlich eine Gruppe ist.

2. Zeigen Sie, dass G genau dann abelsch ist, wenn $G = G^{\mathrm{op}}$ gilt.

3. Zeigen Sie, dass für jede Gruppe G bereits $G \cong G^{\mathrm{op}}$ gilt.

Übung 7. *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 $c \colon G \to \mathrm{Aut}(G)$, $g \mapsto c_g$ ein Gruppenhomomorphismus ist.

3. Zeigen Sie, dass $\ker c = \mathrm{Z}(G)$ gilt.

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.

Übung 8. *Gruppen mit trivialer Automorphismengruppe*
Es sei G eine Gruppe mit trivialer Automorphismengruppe $\mathrm{Aut}(G) = 1$.

1. Zeigen Sie, dass G abelsch ist.

2. Zeigen Sie, dass $2x = 0$ für alle $x \in G$ gilt.

3. Folgern Sie, dass G mit der Struktur eines $\mathbb{F}_2$-Vektorraums versehen werden kann.

4. Bestimmen Sie G bis auf Isomorphie.
   (*Hinweis*: Jeder Vektorraum hat eine Basis.)

Übung 9. *Multiplikativität des Index*
Es sei G eine Gruppe, und es seien $K \subseteq H \subseteq G$ Untergruppen. Zeigen Sie, dass $[G : K] = [G : H][H : K]$ gilt.

Übung 10. *Abelsche Quotienten*
Es sei G eine Gruppe und $N \subseteq G$ eine Untergruppe. Zeigen Sie, dass N genau dann normal in G mit abelschen Quotienten G/N ist, wenn $N \supseteq [G, G]$ gilt.

Übung 11. *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 N 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.
   (*Hinweis*: Betrachten Sie das Bild einer entsprechenden Untergruppe $H \subseteq G$ unter der kanonische Projektion $G \to G/N$.)

5. Entscheiden Sie, ob die vorherige Aussage auch dann noch gilt, wenn N nicht normal in G ist.

Übung 12. *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.

Übung 13. *Untergruppen vom endlichen Index*
Es sei G eine Gruppe und $H \subseteq G$ eine Untergruppe von endlichen Index. Zeigen Sie, dass es eine normale Untergruppe $N \subseteq G$ von endlichen Index mit $N \subseteq H$ gibt.
(*Hinweis*: Konstruieren Sie für $n = [G : H]$ einen Gruppenhomomorphismus $G \to S_n$.)

Übung 14. *Untergruppen von Index* 2
Es sei G eine Gruppe.

1. Es sei $N \subseteq G$ eine Untergruppe vom Index $[G : N] = 2$. Zeigen Sie, dass N bereits normal in G ist.
2. Es sei $H \subseteq G$ eine Untergruppe deren Index $[G : H] =: p$ prim ist. Zeigen Sie, dass H für $p \geq 3$ nicht notwendigerweise prim in G ist.

Übung 15. *Charakteristische Untergruppen*
Eine Untergruppe $H \subseteq G$ einer Gruppe G heißt *charakteristisch*, wenn $\varphi(H) = H$ für jeden Automorphismus $\varphi\colon G \to G$ gilt.

1. Zeigen Sie, dass jede charakteristische Untergruppe $H \subseteq G$ bereits normal ist.
2. Zeigen Sie, dass die Untergruppen $\mathrm{Z}(G), [G, G] \subseteq G$ charakteristisch sind.
3. Es sei $N \subseteq G$ eine normale Untergruppe und $K \subseteq N$ eine charakteristische Untergruppe. Zeigen Sie, dass die Untergruppe K bereits normal in G ist.
4. Folgern Sie, dass für jede normale Untergruppe $N \subseteq G$ auch das Zentrum $\mathrm{Z}(N)$ normal in G ist.

Übung 16. *Gruppen in denen alles Primordnung hat*
Es sei G eine Gruppe.

1. Es gelte $g^2 = 1$ für alle $g \in G$. Zeigen Sie, dass G bereits abelsch ist.
2. Es sei p prim mit $p \geq 3$ und es gelte $g^p = 1$ für alle $g \in G$. Entscheiden Sie, ob G notwendigerweise abelsch ist.

Übung 17. 5/8 *an Kommutativität*
Es sei G eine Gruppe.

1. Zeigen Sie, dass G abelsch ist, wenn $G/\mathrm{Z}(G)$ zyklisch ist. (Insbesondere gilt dann bereits $\mathrm{Z}(G) = G$ und somit tatsächlich schon $G/\mathrm{Z}(G) = 1$.)

Von nun an sei G endlich.

2. Zeigen Sie, dass mindestens $3/4$ aller $x \in G$ nicht zentral sind, wenn G nicht abelsch ist. (Ein Element $x \in G$ heißt *zentral* (*in* G), wenn $x \in \mathrm{Z}(G)$ gilt.)

3. Zeigen Sie, dass für jedes $x \in G$ der Zentralisator $Z_G(x) = \{y \in G \mid yx = xy\}$ eine Untergruppe von G ist. Folgern Sie, dass mindestens die Hälfte aller $y \in G$ nicht mit x kommutiert, wenn x nicht zentral ist.

4. Folgern Sie, dass mindestens $3/8$ aller Paare $(x, y) \in G \times G$ nicht kommutieren (d.h. dass $xy \neq yx$ gilt) wenn G nicht abelsch ist.

Kommutieren zwei (gleichverteilt) zufällige Elemente $x, y \in G$ mit einer Wahrscheinlichkeit von mehr als $5/8$, so ist G also bereits abelsch.

Übung 18. *Grundbegriffe der Gruppenwirkungen*
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.

Übung 19. *Vereinigung von Konjugaten*
Es sei G eine endliche Gruppeu und $H \subsetneq G$ eine echte Untergruppe. Zeigen Sie, dass G nicht die Vereinigung der Konjugate von H ist, d.h. dass $G \neq \bigcup_{g \in G} gHg^{-1}$ gilt.

Übung 20. *Wirkung von p-Grupppen*
Es sei G eine endliche p-Gruppe.

1. Die Gruppe G wirke auf einer endlichen Menge X. Zeigen Sie, dass

$$|X| \equiv |X^G| \pmod{p}$$

   gilt. Folgern Sie ferner, dass diese Wirkung einen Fixpunkt besitzt, falls $p \nmid |X|$ gilt.

2. Es sei $G \neq 1$.
   a) Zeigen Sie, dass $\mathrm{Z}(G) \neq 1$ gilt.
   (*Hinweis*: Betrachten Sie eine passende Wirkung von G auf sich selbst.)
   b) Zeigen Sie allgemeiner, dass für jede normale Untergruppe $N \subseteq G$ mit $N \neq 1$ bereits $N \cap \mathrm{Z}(G) \neq 1$ gilt.

3. Zeigen Sie, dass die Anzahl der nicht-normalen Untergruppen von G ein Vielfaches von p ist.
   (*Hinweis*: Betrachten Sie eine passende Wirkung von G auf einer passenden Menge.)

Übung 21. *Ein wenig Sylow*
Es sei G eine endliche Gruppe, $H \subseteq G$ eine Untergruppe und p prim.

1. Es sei P eine p-Sylowuntergruppe von G mit $P \subseteq H$. Zeigen Sie, dass P auch eine p-Sylowuntergruppe von H.

2. Es sei P eine p-Sylowuntergruppe von H. Zeigen Sie, dass es eine p-Sylowuntergruppe P' von G mit $P = H \cap P'$ gibt.

3. Folgern Sie: Falls G eine normale p-Sylowuntergruppe enthält, so enthält auch H eine normale P-Sylowuntergruppe.

4. Folgern Sie außerdem: Ist H normal in G und P eine p-Sylowuntergruppe von G, so ist $H \cap P$ eine p-Sylowuntergruppe von H ist.

5. Es seien $P, P' \subseteq G$ zwei p-Sylowuntergruppen mit $P' \subseteq N_G(P)$. Zeigen Sie, dass bereits $P = P'$ gilt.

6. Es sei P eine p-Sylowuntergruppe von G mit $N_G(P) \subseteq H$. Zeigen Sie, dass dann $N_G(H) = H$ gilt. Folgern Sie, dass $N_G(N_G(P')) = N_G(P')$ für jede p-Sylowuntergruppe P' von G gilt.

Übung 22. *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.

Übung 23. *Bahnen zählen*
Eine endliche Gruppe G wirke auf einer endlichen Menge X. Für jedes $g \in G$ sei $\mathrm{Fix}(g) \coloneqq \{x \in X \mid g.x = x\}$ die Menge der Fixpunkte von g. Zeigen Sie, dass

$$\frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)| = |X/G|$$

gilt. (Die durchschnittliche Anzahl der Fixpunkte ist also die Anzahl der Bahnen.)

Übung 24. *Genau zwei Konjugationsklassen*
Eine endliche Gruppe G wirke auf einer Menge X.

1. Zeigen Sie, dass für jedes $x \in X$ die Kardinalität $|G.x|$ der Bahn $G.x$ ein Teiler der Gruppenordnung $|G|$ ist.

2. Es sei G eine Gruppe mit genau zwei Konjugationsklassen. Zeigen Sie, dass bereits $G \cong \mathbb{Z}/2$ gilt.

Übung 25. *Zur Kommutativität von* $\mathrm{GL}_n(K)$

Bestimmen Sie alle Körper K und natürliche Zahlen $n \geq 1$, so dass die Gruppe $\mathrm{GL}_n(K)$ abelsch ist.

Übung 26. *Die oberen* 2×2*-Matrizen*

Es sei K ein Körper.

1. Zeigen Sie, dass
$$\mathrm{B}_2(K) \coloneqq \left\{ \begin{pmatrix} a_1 & b \\ 0 & a_2 \end{pmatrix} \middle| a_1, a_2 \in K^\times, b \in K \right\}.$$
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
$$\mathrm{U}_2(K) \coloneqq \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \middle| b \in K \right\}.$$
eine normale Untergruppe von $\mathrm{B}_2(K)$ ist, und dass $\mathrm{B}_2(K)/\mathrm{U}_2(K) \cong K^\times \times K^\times$ gilt.
4. Entscheiden Sie, ob $\mathrm{B}_2(K) \cong \mathrm{U}_2(K) \times K^\times \times K^\times$ gilt.

Übung 27. *Vereinigung von Untergruppen*

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

Übung 28. *Zur Auflösbarkeit von Gruppen*

1. Es sei G eine Gruppe und $N \subseteq G$ eine normale Untergruppe. Zeigen Sie, dass die G genau dann auflösbar ist, wenn die beiden Gruppen N und G/N auflösbar sind.
2. Folgern Sie, dass jede Gruppe der Ordnung pq mit $p \neq q$ prim auflösbar ist.
3. Folgern Sie damit ferner, dass jede Gruppe der Ordnung 30 auflösbar ist.

Übung 29. *Produkte von Normalteilern und auflösbaren Gruppen*
Es seien G_1 und G_2 zwei Gruppen.

1. Es seien $N_1 \subseteq G_1$ und $N_2 \subseteq G_2$ zwei normale Untergruppen. Zeigen Sie, dass auch $N_1 \times N_2 \subseteq G_1 \times G_2$ eine normale Untergruppe ist, und dass
$$(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2)$$
gilt.
2. Folgern Sie, dass $G_1 \times G_2$ auflösbar ist, wenn G_1 und G_2 auflösbar sind.

Übung 30. *Elemente von Ordnung p in p-Gruppen*
Es sei p prim und G eine endliche abelsche p-Gruppe.

1. Zeigen Sie ohne Verwendung der Sylowsätze, dass es eine Untergruppe $H \subseteq G$ vom Index $[G : H] = p$ gibt, falls $G \neq 0$ gilt.
2. Folgern Sie, dass es eine Normalenreihe
$$0 = G_0 \subsetneq G_1 \subsetneq G_2 \subsetneq \cdots \subsetneq G_n = G$$
mit Faktoren $G_i/G_{i-1} \cong \mathbb{Z}/p$ für alle $i = 1, \ldots, n$ gibt.

Übung 31. *Quadrate in endlichen Körpern*
Es sei $p > 0$ prim, n eine positive natürliche Zahl und
$$\mathrm{Quad}(p, n) = \{x^2 \mid x \in \mathbb{F}_{p^n}\}$$
die Menge der Quadrate in $\mathbb{F}_{p^n}$.

1. Bestimmen Sie die Anzahl der Elemente von $\mathrm{Quad}(p, n)$ in Abhängigkeit von p.
2. Entscheiden Sie, für welche p und n die Menge $\mathrm{Quad}(p, n)$ eine Untergruppe der additiven Gruppe von $\mathbb{F}_{p^n}$ ist.
3. Zeigen Sie dass $xy \in \mathrm{Quad}(p, n)$ für alle $x, y \in \mathbb{F}_{p^n}$ mit $x, y \notin \mathrm{Quad}(p, n)$ gilt. (Das Produkt zweier Nicht-Quadrate ist also ein Quadrat.)

Übung 32.
Es sei K ein Körper. Zeigen Sie, dass die Gruppen $(K, +)$ und $(K^\times, \cdot)$ nicht zueinander isomorph sind.

Übung 33. *Flaggen*

Es sei K ein Körper und $n \geq 1$. Eine *Flagge* in K^n ist eine Folge $(V_1, \ldots, V_n)$ von Untervektorräumen $V_i \subseteq K^n$ mit

$$0 \subsetneq V_1 \subsetneq V_2 \subsetneq \cdots \subsetneq V_n = K^n \,.$$

Inbesondere gilt $\dim V_i = i$ für alle i. Es sei $\mathcal{F}(n, K)$ die Menge alle Flaggen in K^n und $S \coloneqq (\langle e_1 \rangle, \langle e_1, e_2 \rangle, \ldots, \langle e_1, \ldots, e_n \rangle = K^n)$ die *Standardflagge* in K^n.

1. Zeigen Sie: Die Gruppe $\mathrm{GL}_n(K)$ wirkt auf der Menge $\mathcal{F}(n, K)$ vermöge

   $$A.(V_1, \ldots, V_n) = (AV_1, \ldots, AV_n)$$

   für alle $A \in G$, $(V_1, \ldots, V_n) \in \mathcal{F}(n, K)$. (Für alle $A \in \mathrm{GL}_n(K)$, $X \subseteq K^n$ ist dabei $SX = \{Sx \mid x \in X\}$.)

2. Zeigen Sie, dass diese Wirkung transitiv ist.

3. Zeigen Sie, dass der Stabilisator der Standardflagge S durch die Gruppe der oberen Dreiecksmatrizen $\mathrm{B}_n(K)$ gegeben ist.

4. Folgern Sie für den endlichen Körper $\mathbb{F}_q$ mit q Elementen, dass

   $$|\mathcal{F}(n, \mathbb{F}_q)| = \prod_{k=0}^{n-1} (1 + q + \cdots + q^k) \,.$$

2 Ringtheorie

Übung 34. *Wahr oder Falsch?*
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. Für alle Ringe R_1 und R_2 gilt $(R_1 \times R_2)[X] \cong R_1[X] \times R_2[X]$.
5. Jeder faktorielle Ring ist unendlich.
6. Für jeden kommutativen Ring R gibt es einen Integritätsbereich S, so dass $R \cong S/I$ für ein Ideal $I \subseteq S$.
7. Jeder endliche Integritätsbereich ist ein Hauptidealring.
8. Ist R ein endlicher kommutativer Ring, so ist $R[X, Y]$ noethersch.
9. Ist R ein Hauptidealring, so ist auch $R[X]$ ein Hauptidealring.
10. Ist R ein Integritätsbereich und $p \in R$ prim, so ist p irreduzibel.
11. Sind $n_1, n_2, n_3 \in \mathbb{Z}$ mit $\mathrm{ggT}(n_1, n_2, n_3) = 1$, so hat das Gleichungssystem

$$\begin{cases} x & \equiv & a_1 & \mod n_1, \\ x & \equiv & a_2 & \mod n_2, \\ x & \equiv & a_3 & \mod n_3, \end{cases}$$

    für alle $a_1, a_2, a_3 \in \mathbb{Z}$ eine Lösung.
12. Ist R ein endlicher kommutativer Ring mit $p \coloneqq \operatorname{char} R > 0$ prim, so ist die Abbildung $R \to R$, $x \mapsto x^p$ ein Ringautomorphismus.

Übung 35. *Irreduziblität von Polynomen*
Entscheiden Sie, ob die folgenden Polynome jeweils irreduzibel sind:

1. $f(X) \coloneqq X^3 - 2 \in \mathbb{Z}[X]$.
2. $f(X) \coloneqq X^3 + 39X^2 - 4X + 8 \in \mathbb{Z}[X]$.
3. $f(X) \coloneqq (X - 3)^2 + 1 \in \mathbb{Q}[X]$.
4. $f(X) \coloneqq 2X^3 - 14X + 2 \in \mathbb{Q}[X]$.
5. $f(X) \coloneqq 2X^3 - 14X + 2 \in \mathbb{Z}[X]$.
6. $f(X) \coloneqq X^3 - 18X^2 + 6X + 3 \in \mathbb{Q}[X]$.

7. $f(X) \coloneqq X^3 - 18X^2 + 6X + 3 \in \mathbb{R}[X]$.
8. $f(X) \coloneqq X^5 + 15X^2 + 6X + 21 \in \mathbb{Z}[X]$.
9. $f(X) \coloneqq X^3 + 2X^2 + X + 1 \in \mathbb{Z}[X]$.
10. $f(X) \coloneqq 2X^4 + 200X^3 + 2000X^2 + 20000X + 20 \in \mathbb{Q}[X]$.
11. $f(X) \coloneqq X^n - t \in K(t)[X]$ für einen Körper K und $n \geq 1$.
12. $f(X, Y) \coloneqq XY^3 + X^2Y + 3XY^2 + X^2 + 3XY + 2X + Y + 2 \in \mathbb{Q}[X]$.
13. $f(X, Y) \coloneqq X^3 + Y^3 + X^2Y + XY^2 + XY + 6X + 6Y + 3 \in \mathbb{Q}[X, Y]$.
14. $f(X) \coloneqq X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Q}[X]$ für $p > 0$ prim.
15. $f(X) \coloneqq X^n + X^{n-1} + \cdots + X + 1 \in \mathbb{Q}[X]$ für $n \geq 3$ ungerade.
16. $f(X) \coloneqq X^6 + X^3 + 1 \in \mathbb{Q}[X]$.
17. $f(X) \coloneqq 2X^5 - 87X^3 + 3X^2 + 21X - 96 \in \mathbb{Q}[X]$.
18. $f(X) \coloneqq X^3 + 2X^2 - 3X + 5 \in \mathbb{Q}[X]$.
19. $f(X) \coloneqq X^4 + 1 \in \mathbb{Q}[X]$.

Übung 36. *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) $t^3 + t^2 + t + 1, t^2 - 1, t^3 - t^2 + t - 1 \in \mathbb{Q}[t]$

Übung 37. *Inverse in Quotienten*
Bestimmen Sie jeweils das Inverse von

1. 13 in $\mathbb{Z}/29$,
2. 231 in $\mathbb{Z}/820$,
3. 99 in $\mathbb{Z}/2345$,
4. t^4+1 in $\mathbb{Q}[t]/(t^5-1)$,
5. t^3-1 in $\mathbb{Q}[t]/(t^3+t^2+t+1)$,
6. t^3+t+1 in $\mathbb{Q}[t]/(t^4+t+1)$.

Übung 38. *Simultane Kongruenzen*
Bestimmen Sie alle Lösungen der folgenden Systeme simultaner Kongruenzen:

1. $\begin{cases} 5x \equiv 6 \mod 12, \\ 3x \equiv 7 \mod 11, \end{cases}$ mit $x \in \mathbb{Z}$.
2. $\begin{cases} 2x \equiv 1 \mod 3, \\ 3x \equiv 2 \mod 5, \\ 5x \equiv 3 \mod 7, \end{cases}$ mit $x \in \mathbb{Z}$.
3. $\begin{cases} 2x \equiv 6 \mod 11, \\ 3x \equiv 7 \mod 14, \\ 4x \equiv 8 \mod 15, \end{cases}$ mit $x \in \mathbb{Z}$.
4. $\begin{cases} (t+1)p \equiv 2 \mod t+2, \\ (t-1)p \equiv 3 \mod t-2, \end{cases}$ mit $p \in \mathbb{Q}[t]$.

Übung 39. *Isomorphiepuzzle*
Bestimmen Sie, welche der folgenden sieben Ringe isomorph zueinander sind, und welche nicht:

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

Übung 40. *Vereinfachung von Quotienten*
Bestimmen Sie für die folgenden Ringe jeweils die Anzahl der Elemente, Einheiten und nilpotenten Elemente.

1. $\mathbb{Z}[X]/(5, 10X^4 - 3X^3 + 8X - 11)$
2. $\mathbb{Z}[X]/(3, 4X^3 + 13X^2 + 10X - 5)$

3. $\mathbb{Z}[X]/(7, 3X^2 + 7X - 14)$

Übung 41.
Es sei R ein Ring. Konstruieren Sie eine Bijektion zwischen R und der Menge der Ringhomomorphismen $\mathbb{Z}[T] \to R$.

Übung 42. *Die einzigen Ringhomomorphismen $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$*
Zeigen Sie, dass die beiden Projektionen $\pi_i \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ mit $\pi_1(x_1, x_2) = x_i$ für alle $(x_1, x_2) \in \mathbb{Z} \times \mathbb{Z}$ die einzigen beiden Ringhomomorphismen $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ sind.

Übung 43.
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.

Übung 44. *Die Eulersche Phi-Funktion*
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 jede Primzahl p und alle $r \geq 1$.
4. Berechnen Sie $\varphi(42)$, $\varphi(57)$ und $\varphi(144)$.

Übung 45. *Polynomringe sind keine Körper*
Zeigen Sie, dass es keinen Ring R gibt, so dass $R[X]$ ein Körper ist.

Übung 46. *Ein nicht-faktorieller Ring*
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 sich jedes Element aus R als Produkt irreduzibler Elemente schreiben lässt.
3. Zeigen Sie, dass R nicht faktoriell ist.
   (*Hinweis*: Zeigen Sie zunächst, dass t^2 und t^3 irreduzibel sind.)

Übung 47. *Charakterisierung von Primidealen*
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.

Übung 48. *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 bereits $Z \cong \mathbb{Z}$ gilt.

Übung 49. *Assoziiertheit in Ringen*

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 $(a) = (b)$ gilt.

Übung 50. *Funktorialität der Einheitengruppe*

Ist R ein kommutativer Ring, so ist

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

die *Einheitengruppe* von R. Zeigen Sie:

1. Zusammen mit der Multiplikation aus R bildet $R^\times$ 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.

Bemerkung. Die Aussagen aus Übung 50 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. So gilt beispielsweise $\mathrm{Mat}_n(R)^\times = \mathrm{GL}_n(R)$. Es genügt auch, dass es $s, t \in R$ mit $rs = 1 = tr$ gibt; dann gilt bereits $s = trs = t$.

Übung 51. *Charakterisierung on Primidealen und maximalen Idealen durch ihre Quotienten*
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.

Übung 52. *Urbilder von Idealen*
Es seien R und S zwei kommutative Ringe und es sei $\phi\colon R \to S$ 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.

Übung 53. *Ideale in Quotienten*
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

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

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

Übung 54. *Noethersch und Hauptidealring für Quotienten*
Es sei R ein Ring und $I \subseteq R$ ein Ideal.

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

Übung 55. *Einheiten in Quotienten*

1. Zeigen Sie für $n \in \mathbb{Z}$ und $q \in \mathbb{Z}$, 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, $I \subseteq R$ ein Ideal und $x \in R$, so ist $\overline{x} \in R/I$ genau dann eine Einheit, wenn $(x) + I = R$.

Übung 56. *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.

Übung 57. *Radikale*

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

1. Definieren Sie das Radikal $\sqrt{I}$.
2. Zeigen Sie, dass $\sqrt{I}$ ein Ideal ist, und dass $I \subseteq \sqrt{I}$ gilt.
3. Zeigen Sie, dass $\sqrt{\sqrt{I}} = \sqrt{I}$.
4. Zeigen Sie, dass $\sqrt{I}$ genau dann ein echtes Ideal ist, wenn I ein echtes Ideal ist.
5. Zeigen Sie für jedes weitere Ideal $J \subseteq R$ die Gleichheit $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

Das Ideal I ist ein *Radikalideal*, wenn es ein Ideal $J \subseteq R$ mit $I = \sqrt{J}$ gibt.

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

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

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

Übung 58. *Gegenbeispiele*

Es sei K ein Körper.

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

Übung 59. *Euklidische Ringe sind Hauptidealringe*
Es sei R ein euklidischer Ring. Zeigen Sie, dass R ein Hauptidealring ist.

Übung 60. *Primideale in Hauptidearingen*
Es sei R ein Hauptidealring. Zeigen Sie, dass jedes Primideal $\mathfrak{m} \subseteq R$ mit $\mathfrak{m} \neq 0$ bereits ein maximales Ideal ist.

Übung 61. *Polynomringe als Hauptidealringe*
Es sei K ein kommutativer Ring, so dass $K[X]$ ein Hauptidealring ist. Zeigen Sie, dass K bereits ein Körper ist.

Übung 62. *Nilpotente zu Einheiten*
Es sei R ein kommutativer Ring.

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

Übung 63. *Die Einheitengruppe des Potenzreihenrings*
Es sei R ein kommutativer Ring. Zeigen Sie, dass

$$R[\![T]\!]^\times = \left\{ \sum_{i=0}^{\infty} f_i T^i \in R[\![T]\!] \,\middle|\, f_0 \in R^\times \right\}.$$

Übung 64. *Einheitengruppe der Gaußschen Zahlen*
Bestimmen Sie die Einheitengruppe $\mathbb{Z}[i]^\times$.

Übung 65. *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 66. *Der Frobeniushomomorphismus*
Es sei R ein kommutativer Ring, so dass $p := \operatorname{char} R > 0$ prim ist.

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.

Übung 67. *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 $s_1, s_2 \in S$ gelten 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.

Übung 68. *Koeffizientenideale in Polynomringen*
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 Menge
$$\mathfrak{a}[X] \coloneqq \left\{ \sum_i f_i X^i \in R[X] \;\middle|\; f_i \in \mathfrak{a} \text{ für alle } i \right\}$$
ein Ideal in $R[X]$ ist.
2. Zeigen Sie, dass die Abbildung
$$R[X]/\mathfrak{a}[X] \to (R/\mathfrak{a})[X], \quad \overline{\sum_i f_i X^i} \mapsto \sum_i \overline{f_i} X^i$$
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 $(\mathfrak{a})_{R[X]} = \mathfrak{a}[X]$ gilt.

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

6. Veinfachen Sie für die folgenden Ringe R und Ideale $I \subseteq R$ jeweils den Quotienten R/I. Entscheiden Sie jeweils anschließend, ob das Ideal prim oder maximal ist.
$$(7) \subseteq \mathbb{Z}[X], \quad (3, X^2+1) \subseteq \mathbb{Z}[X], \quad (5, X^2+6X-2) \subseteq \mathbb{Z}[X], \quad (X^2+1) \subseteq \mathbb{Q}[X,Y].$$

Übung 69. *Produkte von Idealen*
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.

Übung 70. *Ideale in Produkten*
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.

Bemerkung. Übung 69 und Übung 70 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 71. *Lokalisierung und Produkte*
Es seien R und R' zwei kommutative Ringe, und $S \subseteq R$ und $S' \subseteq R'$ multiplikative Teilmengen. Es seien $i\colon R \to R_S$ und $i'\colon R' \to R'_{S'}$ die kanonischen Ringhomomorphismen.

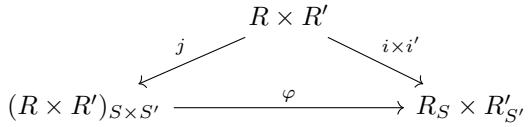
1. Zeigen Sie, dass $S \times S' \subseteq R \times R'$ eine multiplikative Teilmenge ist.

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

2. Zeigen Sie, dass es eine eindeutigen Ringhomomorphismus

$$\varphi\colon (R \times R')_{S \times S'} \to R_S \times R'_{S'}$$

gibt, so dass das folgende Diagram kommutiert:



3. Zeigen Sie, dass φ ein Isomorphismus ist.

Übung 72. *Funktorialität von Lokalisierung*
Es sei $f\colon R \to R'$ ein Ringhomomorphismus zwischen kommutativen Ringen R und R'. Es sei $S \subseteq R$ eine multiplikative Menge.

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

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

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

   Hierbei bezeichnen i und i' jeweils die kanonischen Ringhomomorphismen.

Übung 73. *Lokalisierung durch Quotienten*
Es sei R ein kommutativer Ring und $f \in R$. Zeigen Sie, dass $R_f \cong R[X]/(fX-1)$ gilt. (Dabei ist $R_f = S_f^{-1}R$ für die multiplikative Menge $S_f = \{1, f, f^2, \dots\} = \{f^n \mid n \in \mathbb{N}\}$.)

Übung 74. *Idealtheoretische Beschreibung größter gemeinsamer Teiler*
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 $(a_i \mid i \in I) = (a)$ gilt.

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

Übung 75. *Euklid*
Es sei K ein Körper. Zeigen Sie, dass es in $K[X]$ unendlich viele normierte, irreduzible Polynome gibt.

Übung 76. *Zur Existenz von maximalen Idealen*
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 $I \subseteq \mathfrak{m}$ gilt.

Übung 77. *Der Hilbertsche Basissatz*
Formulieren und beweisen Sie den Hilbertschen Basissatz.

Übung 78. *$K[\![X]\!]$ ist lokal*
Es sei K ein Körper. Zeigen Sie, dass der Ring $K[\![X]\!]$ ein eindeutiges maximales Ideal besitzt.

3 Körpertheorie

Übung 79. *Wahr oder Falsch?*

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.
4. Sind $M/L/K$ Körpererweiterungen, so dass M/L und L/K normal sind, so ist auch M/K normal.
5. Es gilt $\mathbb{F}_8 \subseteq \mathbb{F}_{32}$.
6. Ist L/K eine Körpererweiterung und $\overline{L} \supseteq L$ ein algebraischer Abschluss, so ist auch $\overline{L} \supseteq K$ auch ein algebraischer Abschluss.
7. Ist L/K ein Körperweiterung und L der Zerfällungskörper eines Polynoms $f \in K[X]$ von Grad $n \coloneqq \deg f$, so gilt $[L : K] \mid n!$.
8. Ist L/K ein Körperweiterung und L der Zerfällungskörper eines Polynoms $f \in K[X]$ von Grad $n \coloneqq \deg f$, so gilt $|\mathrm{Gal}(L/K)| \mid n!$.
9. Es sei L/K eine Körpererweiterung und $L_1, L_2 \subseteq L$ seien Unterkörper, so dass die Erweiterungen L_1/K und L_2/K algebraisch sind. Bezeichnet $L_1L_2 \subseteq L$ den kleinsten Unterkörper, der L_1 und L_2 enthält, so ist auch die Erweiterung L_1L_2/K algebraisch.

Übung 80. *Gemeinsame Nullstellen irreduzibler Polynome*

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.

Übung 81. *Rechnen in zyklischen Erweiterungen*

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.

Übung 82. *Erweiterungen vom primer Ordnung*

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

Übung 83. *Zum Grad*

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

2. 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.

Übung 84. *Algebraizität von Summe und Produkt*

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.

Übung 85. *Die Erweiterung* $\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q}$

Es sei $L \coloneqq \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

1. Zeigen Sie, dass $\sqrt{2}, \sqrt{3} \in L$ und folgern Sie, dass $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ gilt.

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.

Übung 86. *Galoisgruppe von* $\mathbb{Q}(\sqrt[3]{3}, \zeta)/\mathbb{Q}$

Es sei $\zeta \in \mathbb{C}$ eine dritte primitive Einheitswurzel (etwa $\zeta = e^{2\pi i/3}$) und $L \coloneqq \mathbb{Q}(\sqrt[3]{3}, \zeta)$.

1. Zeigen Sie, dass $L/\mathbb{Q}$ Galoisch ist.

2. Bestimmen Sie den Grad $[L : \mathbb{Q}]$.

3. Bestimmen Sie die Gruppe $\mathrm{Gal}(L/\mathbb{Q})$ und entscheiden Sie, ob sie abelsch ist.

Übung 87. *Galoisgruppe von* $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$

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

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

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

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

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

Übung 88. *Galoisgruppe von $X^3 - 2X^2 - X + 1$*
Es sei $f(X) \coloneqq X^3 - 2X^2 - X + 1 \in \mathbb{Q}[X]$ 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.

Übung 89. *Produkt von Linearfaktoren*
Es sei K ein Körper und L/K eine endliche Galoiserweiterung. Es sei $f \in K[X]$ und es seien $\alpha_1, \ldots, \alpha_n \in L$ die paarweise verschiedenen Nullstellen von f. Zeigen Sie für das Polynom $g(X) \coloneqq \prod_{i=1}^{n}(X - \alpha_i) \in L[X]$, dass bereits $g \in K[X]$ gilt.
(*Hinweis*: Überlegen Sie sich, dass die Koeffizienten von g invariant unter der Galoisgruppe $\mathrm{Gal}(L/K)$ sind.)

Übung 90. *Galoisgruppe von $\mathbb{R}/\mathbb{Q}$*
Es sei $\sigma \in \mathrm{Gal}(\mathbb{R}/\mathbb{Q})$.

1. Zeigen Sie, dass für alle $x \in \mathbb{R}$ genau dann $x \geq 0$ gilt, wenn $\sigma(x) \geq 0$ gilt.
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 $\mathrm{Gal}(\mathbb{R}/\mathbb{Q}) = 1$.

Übung 91. *Galoisgruppe von $X^p - 2$*
Es sei p eine Primzahl und $f(X) \coloneqq X^p - 2 \in \mathbb{Q}[X]$. Es sei $\zeta \in \mathbb{C}$ eine primitive p-te Einheitswurzel (etwa $\zeta = e^{2\pi i/p}$). Es sei $L \coloneqq \mathbb{Q}(\sqrt[p]{2}, \zeta)$.

1. Zeigen Sie, dass L ein Zerfällungskörper von f ist.
2. Folgern Sie, dass $L/\mathbb{Q}$ galoisch ist.
3. Zeigen Sie, dass $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$ gilt.
   (*Hinweis*: Man betrachte Übung 35.)
4. Folgern Sie, dass $[L : \mathbb{Q}] = p(p-1)$ gilt.
   (*Hinweis*: Zeigen Sie, dass $p, p-1 \mid [L : \mathbb{Q}]$ gilt.)
5. Bestimmen Sie $\mathrm{Gal}(L/\mathbb{Q})$.
6. Entscheiden Sie in Abhängigkeit von p, ob $\mathrm{Gal}(L/\mathbb{Q})$ abelsch ist.
7. Entscheiden Sie in Abhängigkeit von p, ob $\mathrm{Gal}(L/\mathbb{Q}(\sqrt[p]{2}))$ normal in $\mathrm{Gal}(L/\mathbb{Q})$ ist.

8. Entscheiden Sie in Abhängigkeit von p, ob $\mathrm{Gal}(L/\mathbb{Q}(\zeta))$ normal in $\mathrm{Gal}(L/\mathbb{Q})$ ist.

Übung 92. *Charakterisierung von Körpern*
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.

Übung 93. *Unendlichkeit algebraisch abgeschlossener Körper*
Es sei K ein algebraisch abgeschlossener Körper. Zeigen Sie, dass K unendlich ist.

Übung 94. *Irreduziblität quadratischer und kubischer Polynome*
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.

Übung 95. *Abgeschlossenheit algebraischer abgeschlossener Körper*
Es sei K ein algebraisch abgeschlossener Körper und L/K eine algebraische Körpererweiterung. Zeigen Sie, dass bereits $L = K$ gilt.

Übung 96. *Algebraischen Abschlüsse von Unterkörpern*
Es sei L/K eine Körpererweiterung und $\overline{L}/L$ ein algebraischer Abschluss von L.

1. Zeigen Sie, dass $\overline{L}/K$ genau dann ein algebraischer Abschluss ist, wenn L/K algebraisch ist.
2. Zeigen Sie, dass es einen Unterkörper $\overline{K} \subseteq \overline{L}$ gibt, so dass $\overline{K} \supseteq K$ gilt und $\overline{K}/K$ ein algebraischer Abschluss ist.
3. Entscheiden Sie, ob der obige Körper $\overline{K}$ eindeutig ist.

Übung 97. *You should be able to do this*
Zeigen Sie, dass endliche Körpererweiterungen algebraisch sind.

Übung 98. *Transitivität von Algebraizität*
Es seien $M/L/K$ Körpererweiterungen, so dass M/L und L/K algebraisch sind. Zeigen Sie, dass auch M/K algebraisch ist.

Übung 99. *Algebraizität von α und β*
Es sei L/K eine Körpererweiterung und es seien $\alpha, \beta \in L$. Zeigen Sie, dass α und β genau dann beide algebraisch über K sind, wenn $\alpha + \beta$ und $\alpha\beta$ beide algebraisch über K sind.

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

Übung 100. *Zur Separablität*
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.

Übung 101. *Grad des Körperkompositums*
Es sei K ein Körper, L/K eine endliche Körpererweiterung und es seien $K \subseteq L_1, L_2 \subseteq L$ zwei Zwischenkörper. Es sei $L_1L_2 \subseteq L$ der kleinste Unterkörper, der L_1 und L_2 enthält.

1. Zeigen Sie für alle $\alpha, \beta \in L$, dass $[K(\alpha, \beta) : K(\alpha)] \leq [K(\beta) : K]$ gilt.
2. Zeigen Sie, dass $[L_1L_2 : L_2] \leq [L_1 : K]$ gilt.
3. Folgern Sie, dass $[L_1L_2 : K] = [L_1 : K][L_2 : K]$ gilt falls $[L_1 : K]$ und $[L_2 : K]$ teilerfremd sind.

Übung 102. *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.

Übung 103. *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/K 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.

Übung 104. *Charakterisierung algebraischer Erweiterungen durch Zwischenringe*
Zeigen Sie, dass eine Körpererweiterung L/K genau dann algebraisch ist, wenn jeder Zwischenring $K \subseteq R \subseteq L$ bereits ein Körper ist.

Übung 105. *Charakterisierung galoischer Unterkörper*
Es seien $L/E/K$ endliche Körpererweiterungen, so dass L/K galoisch ist. Zeigen Sie, dass E/K genau dann galoisch ist, wenn $\sigma(E) = E$ für alle $\sigma \in \mathrm{Gal}(L/K)$ gilt.

4 Modultheorie

Übung 106. *Wahr oder Falsch?*
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. Es gilt $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2, \mathbb{Z}/3) = 0$.
4. 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.
5. Ist M ein freier R-Modul und $S \subseteq R$ ein Unterring, so ist M auch als S-Modul frei.
6. Ist M ein freier R-Modul endlichen Rangs, so ist auch jeder Untermodul $N \subseteq M$ frei.
7. Ist jeder R-Modul frei, so ist R ein Körper.
8. Ist M ein R-Modul und $N \subseteq M$ ein Untermodul, so gibt es einen Untermodul $P \subseteq M$ mit $M = N \oplus P$.
9. Sind M und N zwei freie R-Moduln endlichen Rangs, so ist auch $\mathrm{Hom}_R(M, N)$ ein freier R-Modul endlichen Rangs.
10. Ist M ein endlich erzeugter R-Modul, so ist auch jeder Untermodul $N \subseteq M$ endlich erzeugt.
11. 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.
12. Ist M ein endlich erzeugter R-Modul und $E \subseteq M$ ein minimales Erzeugendensystem, so ist E endlich.
13. 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.
14. 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.
15. Ist R ein Hauptidealring, so spaltet jede kurze exakte Sequenz von endlich erzeugten torsionsfreien R-Moduln.
16. Ist P ein projektiver R-Modul, so gibt es einen R-Moduln C, so dass $P \oplus C$ frei ist.
17. 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 $M_1/N_1 \cong M_2/N_2$.

18. Ist M ein R-Modul mit $M \cong M \oplus M$, so gilt $M = 0$.

Übung 107. *Herleitung der Jordannormalform*

1. Formulieren Sie den Hauptsatz über endlich erzeugte Moduln über Hauptidealringen.
2. Leiten Sie aus obigen Satz die Existenz der Jordannormalform über algebraisch abgeschlossenen Körpern her.

Übung 108. *Abelsche Gruppen endlicher Ordnung*

Bestimmen Sie bis auf Isomorphie alle abelschen Gruppen der Ordnung

1. 213
2. 675,
3. 3087,
4. 152460.

Übung 109. *Smith-Normalform Und Kokerne*

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

$$A_1 = \begin{pmatrix} 38 & -12 \\ 18 & -6 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 10 & 8 \\ -2 & 6 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 8 & 8 & -2 \\ 10 & 2 & 2 \end{pmatrix},$$
$$A_4 = \begin{pmatrix} 1 & 2 & 3 \\ -2 & 3 & 1 \\ 3 & 2 & 1 \end{pmatrix}, A_5 = \begin{pmatrix} 2 & 4 & 6 \\ 4 & 3 & 7 \\ 11 & -2 & 3 \end{pmatrix}, \quad A_6 = \begin{pmatrix} 15 & 11 & 10 \\ 3 & 2 & -2 \\ 15 & 10 & 11 \end{pmatrix},$$
$$A_7 = \begin{pmatrix} -1 & 1 & 0 \\ -2 & -2 & 1 \\ 2 & -2 & 0 \\ -1 & -1 & 3 \end{pmatrix}.$$

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

$$A_8 = \begin{pmatrix} t^2 & t^4 - t^2 \\ t & t^2 - t \end{pmatrix}, \quad A_9 = \begin{pmatrix} t+1 & 2t^2 - 2t - 2 \\ 2t & 4t^2 - 6t \end{pmatrix}.$$

Übung 110. *Eine Isomorphie von abelschen Gruppen*
Es seien $n, m \geq 1$. Zeigen Sie, dass $\mathbb{Z}/n \oplus \mathbb{Z}/m \cong \mathbb{Z}/\operatorname{ggT}(n,m) \oplus \mathbb{Z}/\operatorname{kgV}(n,m)$.

Übung 111. *Über* $\operatorname{Hom}_R(R, -)$
Es sei R ein kommutativer Ring und M ein R-Modul. Zeigen Sie, dass $\operatorname{Hom}_R(R, M) \cong M$ als R-Moduln.

Übung 112. *Zum Spalten kurzer exakter Sequenzen*
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 $0 \to N \xrightarrow{f} M \xrightarrow{g} F \to 0$ spaltet.

Übung 113. $\mathbb{Q}$ *ist nicht endlich erzeugt*
Zeigen Sie, dass $\mathbb{Q}$ als abelsche Gruppe nicht endlich erzeugt ist.

Übung 114. *Surjektive Endomorphismen noetherscher Moduln*
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 114 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.

Übung 115. *Ein Lemma von Schur*
Ein R-Modul M heißt *einfach*, wenn M genau zwei Untermoduln hat.

1. Zeigen Sie, dass M genau dann einfach ist, wenn $M \neq 0$ gilt 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.

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

Übung 116. $\mathbb{Z}$*-Moduln und abelsche Gruppen*
Zeigen Sie, dass es auf jeder abelschen Gruppe genau eine $\mathbb{Z}$-Modulstruktur gibt.

Übung 117. *Moduln über Lokalisierungen und Quotienten*
Es sei R ein kommutativer Ring und M ein R-Modul. Es sei $I \subseteq R$ ein Ideal und $S \subseteq R$ eine multiplikative Teilmenge.

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

Übung 118. *Jeder Modul ist Quotient eines freien Moduls*
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 $K \subseteq F$ gilt.

Übung 119. *Charakterisierung zyklischer Moduln*
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 $M \cong R/I$ als R-Moduln.

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

Übung 120. *Existenz endlicher Erzeugendensysteme*
Es sei M ein endlich erzeugter R-Modul. Zeigen Sie, dass jedes Erzeugendensystem $E \subseteq M$ ein endliches Erzeugendensystem enthält.

Übung 121. *Idempotente*
Es sei R ein Ring und $e \colon M \to M$ ein idempotenter Endomorphismus eines R-Moduls M, d.h. es gelte $e^2 = e$. Zeigen Sie, das $M = \operatorname{im} e \oplus \ker e$ gilt, und dass $e(m + m') = m$ für alle $m \in \operatorname{im} e$ und $m' \in \ker e$ gilt.

Übung 122. *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-Modul 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.

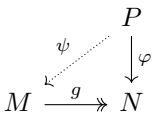
Übung 123. *Äquivalente Charakterisierungen projektiver Moduln*
Es sei R ein Ring und P ein R-Modul. Zeigen Sie, dass die folgenden Bedingungen äquivalent sind:

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

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

   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:

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*.

Übung 124. *Einschränkung kurzer exakter Sequenzen*

Es sei R ein Ring, $0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0$ 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. Dabei bezeichnen $f'\colon f^{-1}(M') \to M'$, $m \mapsto f(m)$ und $g'\colon M' \to g(M')$, $m \mapsto g(m)$ die jeweiligen Einschränkungen von f und g.

Übung 125. *Endlichkeit in kurzen exakten Sequenzen*

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

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

Übung 126. *Charakterisierungen noetherscher Moduln*

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

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

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

   von Untermoduln von M stabilisiert, i.e. es gibt ein $i \geq 0$ mit $N_j = N_i$ für alle $j \geq i$.
3. Jede nicht-leere Menge $\mathcal{S}$ bestehend aus R-Untermoduln von M besitzt ein maximales Element, d.h. ein Element $N \in \mathcal{S}$, das in keinem anderen Element von $\mathcal{S}$ echt enthalten ist.

Übung 127. *Konstruktionen mit noetherschen Moduln*

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

Übung 128. *Untermoduln freier Moduln über Hauptidealringen*

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 128 auf freie Moduln beliebigen Rangs.

Übung 129. *Untermoduln endlich erzeugter Moduln über Hauptidealringen*
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 $m_1, \ldots, m_t \in M$ Entscheiden Sie, ob jeder Untermodul $N \subseteq M$ ein Erzeugendensystem aus $\leq t$ vielen Elementen besitzt.

Übung 130. *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.

Übung 131. *p-primär in kurzen exakten Sequenzen*

Es sei R ein Hauptidealring, $p \in R$ prim und $0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0$ eine kurze exakte Sequenz von R-Moduln. Zeigen Sie, dass M genau dann p-primär ist, wenn N und P beide p-primär sind.

Übung 132. *Produkte und Summen exakter Sequenzen*

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.

Übung 133. *Annihilatoren von Quotienten*
Es sei R ein kommutativer Ring.

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

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.

Übung 134. *Isomorphie von Quotientenringen als Moduln*
Es sei R ein kommutativer Ring und $I, J \subseteq R$ seien zwei Ideale.

1. Zeigen Sie, dass $I = J$ gilt, falls $R/I \cong R/J$ als R-Moduln gilt.
(*Hinweis*: Betrachten Sie Annihilatoren.)
2. Entscheiden Sie, ob die Aussage auch stimmt, wenn $R/I \cong R_J$ als Ringe gilt.

Übung 135. *Rechenregeln für Annihilatoren*
Es sei M ein R-Modul.

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

5. Geben Sie ein Beispiel an, in dem die obige Inklusion strikt ist.

Übung 136. *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 $\bigoplus_{n\in\mathbb{N}} R$.)

5 Lösungen

Lösung 1.

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 $g\left(\bigcap_{i\in I} N_i\right) g^{-1} \subseteq \bigcap_{i\in I}(gN_ig^{-1}) \subseteq \bigcap_{i\in I} N_i$.

3. Die Aussage ist *wahr*: Nach dem chinesischen Restklassensatz gilt

$$\mathbb{Z}/11 \times \mathbb{Z}/13 \cong \mathbb{Z}/(11 \cdot 13) = \mathbb{Z}/143$$

   als Ringe, und somit inbesondere auch als abelsche Gruppen.

4. Die Aussage ist *wahr*: Jede Gruppe der Ordnung 101 ist zyklisch (siehe Übung 11) und somit abelsch (siehe Übung 5).

5. Die Aussage ist *wahr*: Es gilt $G \cong \mathbb{Z}/p$, weshalb G abelsch und somit auflösbar ist.

6. Die Aussage ist *falsch*: Für die Gruppe $G = \mathbb{Z}/4$ und Untergruppe $H = 2\mathbb{Z}/4$ gelten $|H| = 2$ und $|G/H| = |G|/|H| = 4/2 = 2$ und somit $G/H \cong H \cong \mathbb{Z}/2$. Es gilt aber $\mathbb{Z}/4 \ncong \mathbb{Z}/2 \times \mathbb{Z}/2$. (Die rechte Seite enthält kein Element der Ordnung 4.)

7. Die Aussage ist *falsch*: Die Untergruppe $A_3 \subseteq S_3$ ist normal, und da $|A_3| = 3$ und $|S_3/A_3| = |S_3|/|A_3| = 2$ gelten, sind $A_3 \cong \mathbb{Z}/3$ und $S_3/A_3 \cong \mathbb{Z}/2$ abelsch. Aber S_3 ist nicht abelsch.

8. Die Aussage ist *wahr*: Falls es ein Element $g \in G$ unendlicher Ordnung gibt, so gilt $\mathbb{Z} \cong \langle g\rangle \subseteq G$. Dann entspricht die echte Untergruppe $2\mathbb{Z} \subsetneq \mathbb{Z}$ einer echten Untergruppe von G. Ansonsten hat jedes Element $g \in G$ endliche Ordnung, weshalb dann $\langle g\rangle$ eine echte Untergruppe von G ist.

9. Die Aussage ist *falsch*: Die Heisenberg-Gruppe

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{pmatrix} \middle| \, a, b, c \in \mathbb{F}_p \right\}$$

   ist nicht abelsch, da etwa

$$\left(\begin{smallmatrix} 1 & 1 & 0 \\ & 1 & 0 \\ & & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 & 0 \\ & 1 & 1 \\ & & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} 1 & 1 & 0 \\ & 1 & 1 \\ & & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 & 0 \\ & 1 & 1 \\ & & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 & 0 \\ & 1 & 0 \\ & & 1 \end{smallmatrix}\right).$$

10. Die Aussage ist *wahr*: Für alle $i = 1, \ldots, n$ gelten $\rho^{i-1}(1) = i$ und $\rho^{i-1}(2) = i+1$, und somit

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

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

11. Die Aussage ist *wahr*: Mithilfe von Polarkoordinaten ergibt sich, dass $\mathbb{C}^\times \cong \mathbb{R}_{>0} \times S^1$ gilt. Dabei gilt $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$ vermöge der Exponentialfunktion.

12. Die Aussage ist *falsch*: In $\mathbb{C}^\times$ ist jedes Element ein Quadrat. Gleiches gilt dann auch für $\mathbb{C}^\times / H$. Aber $-1 \in \mathbb{R}^\times$ ist kein Quadrat.

13. Die Aussage ist *wahr*: Es gilt

$$2s = s + s = \sum_{a \in A} a + \sum_{a \in A} a = \sum_{a \in A} a + \sum_{a \in A} (-a) = \sum_{a \in A} a - \sum_{a \in A} a = 0\,.$$

14. Die Aussage ist *wahr*: Es gilt

$$\begin{aligned} |\mathrm{GL}_n(\mathbb{F}_p)| &= (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) \\ &= \underbrace{p^{1+2+\cdots+(n-1)}}_{=p^{n(n-1)/2}} \underbrace{(p^n - 1)(p^{n-1} - 1) \cdots (p-1)}_{=:m}\,. \end{aligned}$$

Dabei gilt $p \nmid (p^k - 1)$ für alle $k \geq 1$, und somit auch $p \nmid m$. Die p-Sylowuntergruppen von $\mathrm{GL}_n(\mathbb{F}_p)$ sind deshalb genau die p-Untergruppen der Ordnung $p^{n(n-1)/2}$. Die Gruppe $\mathrm{U}_n(\mathbb{F}_p)$ hat diese Ordnung.

15. Die Aussage ist *wahr*: Die Elemente gh und hg sind konjugiert zueinander durch $g(hg)g^{-1} = gh$.

16. Die Aussage ist *falsch*: Wir geben zwei Gegenbeispiele:
    a) Für alle $\alpha \in \mathbb{R}$ sei

$$r_\alpha \coloneqq \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$$

die Drehung der Ebene $\mathbb{R}^2$ um den Winkel α, und

$$s_\alpha \coloneqq \begin{pmatrix} \cos(2\alpha) & \sin(2\alpha) \\ \sin(2\alpha) & -\cos(2\alpha) \end{pmatrix}.$$

die Spiegelung der Ebene $\mathbb{R}^2$ an der Achse, die zur x-Achse den Winkel α hat. Für alle $\alpha, \beta \in \mathbb{R}$ ist dann

$$s_\alpha s_\beta = r_{2(\alpha-\beta)}$$

die Rotation um den Winkel $2(\alpha - \beta)$.

Es sei $\alpha \in \mathbb{R}$ irrational und es seien $\beta_1, \beta_2 \in \mathbb{R}$ mit $2(\beta_1 - \beta_2) = 2\pi\alpha$, und es sei $G \coloneqq \langle s_{\beta_1}, s_{\beta_2} \rangle$ die von s_{β_1}, s_{β_2} erzeugte Untergruppe von $\mathrm{GL}_2(\mathbb{R})$. Dann wird G von zwei Elementen von Ordnung 2 erzeugt. Aber $r_{2\pi\alpha} = s_{\beta_1} s_{\beta_2} \in G$ hat unendliche Ordnung, da $2\pi\alpha$ ein nicht-rationales Vielfaches von 2π ist. Somit kann G nicht endlich sein.

b) Es sei $S(\mathbb{Z})$ die Symmetriegruppe der Menge der natürlichen Zahlen $\mathbb{Z}$. Es sei $\tau_0, \tau_1 \in S(\mathbb{Z})$ durch

$$\tau_0(n) = -n \quad \text{und} \quad \tau_1(n) = 2 - n$$

gegeben. (Man stelle sich einen unendlichen ungerichteten Graphen vor mit Knotenmenge $\mathbb{Z}$ vor, bei dem es für jeden Knoten $n \in \mathbb{Z}$ genau zwischen n und $n \pm 1$ eine Kante gibt. Dann entsprechen τ_0 und τ_1 die Spiegelungen an den Knoten 0 und 1.) Dann gilt

$$(\tau_1 \circ \tau_0)(n) = \tau_1(\tau_0(n)) = \tau_1(-n) = 2 - (-n) = n + 2\,,$$

weshalb $\tau_0\tau_1$ unendliche Ordnung hat. (Anschaulich gesehen ist $\tau_0\tau_1$ die Verschiebung um zwei Knoten.) Es bezeichne $G \coloneqq \langle \tau_0, \tau_1 \rangle$ die von τ_0 und τ_1 erzeugte Untergruppe von $S(\mathbb{Z})$. Dann hat $\tau_1\tau_0 \in G$ unendliche Ordnung, weshalb G unendlich ist.

Lösung 2.

Nach Annahme gibt es ein $g \in G$ mit $G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$.

1. Für $x, y \in G$ gibt es $a, b \in \mathbb{Z}$ mit $x = g^a$ und $y = g^b$, und deshalb gilt

$$xy = g^a g^b = g^{a+b} = g^{b+a} = g^b g^a = yx.$$

2. Die Abbildung $\varphi\colon \mathbb{Z} \to G$, $n \mapsto g^n$ ist ein Gruppenhomomorphismus, und nach Annahme surjektiv. Für $n \in \mathbb{Z}$ mit $n \geq 0$ und $\ker\varphi = (n)$ induziert deshalb φ einen Isomorphismus

$$\overline{\varphi}\colon \mathbb{Z}/n \to G, \quad \overline{n} \mapsto g^n.$$

Ist G unendlich, so muss $n = 0$ gelten; ist G endlich, so muss $n = |\mathbb{Z}/n| = |G|$ gelten. Das zeigt die Eindeutigkeit von n.

Lösung 3.

1. Da H nichtleer ist, gibt es ein Element $x \in H$. Deshalb $1 = xx^{-1} \in H$. Für jedes $x \in H$ gilt somit auch $x^{-1} = 1 \cdot x^{-1} \in H$. Für alle $x, y \in H$ gilt dann $y^{-1} \in H$, und somit auch $xy = x(y^{-1})^{-1} \in H$. Ingesamt zeigt dies, dass H eine Untergruppe von G ist.

2. Es sei $1_H \in H$ das neutrale Element von H, und es sei $x \in G$ das in G inverse Element zu 1_H. Es gilt $1_H^2 = 1_H$, da 1_H neutral in H ist, und somit

$$1_H = 1_H 1_G = 1_H 1_H x = 1_H^2 x = 1_H x = 1_G\,.$$

Also besitzen H und G das gleiche neutrale Element. (Hier nutzen wir, dass in einer Gruppe K die Identität 1_K das einzige Element $k \in K$ mit $k^2 = k$ ist.) Ist $x \in H$ und $y \in H$ das zu x in H inverse Element, so gilt deshalb $xy = 1_H = 1_G$, weshalb y auch in G invers zu x ist.

Zusammen zeigt dies, dass H bereits eine Untergruppe von G ist.

Lösung 4.

Ist H eine Untergruppe, so gilt per Definition für alle $x, y \in H$ auch $xy \in H$.

Andererseits sei nun $H \subseteq G$ eine entsprechende Teilmenge. Es gibt ein Element $h \in H$, da H nicht leer ist. Da G endlich ist, hat h endliche Ordnung, d.h. es gibt $n \geq 1$ mit $h^n = 1$. Inbesondere gilt $1 = h^n \in H$. Ist $h \neq 1$, so gilt außerdem $n \geq 2$, und somit auch $h^{-1} = h^{n-1} \in H$. Also ist H eine Untergruppe.

Lösung 5.

(i) $\implies$ ii)) Ist G eine Gruppe und sind $a, b \in G$, so gilt für alle $x \in G$, dass genau dann $ax = b$ gilt, wenn $x = a^{-1}b$ gilt, und genau dann $xa = b$ gilt, wenn $x = b^{-1}a$ gilt. Also sind beide Gleichungen eindeutig lösbar.

(iii) $\implies$ ii)) Andererseits seien nun die Gleichungen $ax = b$ und $xa = b$ für alle $a, b \in G$ eindeutig lösbar. Es gibt ein Element $a \in G$, da G nicht leer ist. Nach Annahme gibt es ein Element $e \in G$ mit $ea = a$. Für jedes $b \in G$ gilt dann ebenfalls $eb = b$, denn nach Annahme gibt es ein $c \in G$ mit $ac = b$, und somit gilt

$$eb = eac = ac = b\,.$$

Das zeigt, dass e linksneutral in G ist. Für jedes $a \in G$ gibt es nun nach Annahme ein $b \in G$ mit $ba = e$, also eine Linksinverses zu a.

Lösung 6.

1. Für alle $g \in G^{\mathrm{op}}$ gilt $g * 1_G = 1_G \cdot g = g$, sowie analog auch $1_G * g = g$. Also ist 1_G neutral bezüglich $*$. Für $g \in G$ bezeichne g^{-1} das inverse Element von g in G. Dann gilt $g * g^{-1} = g^{-1} \cdot g = 1_G = 1_{G^{\mathrm{op}}}$, sowie analog auch $g^{-1} * g = 1_{G^{\mathrm{op}}}$. Also ist g^{-1} auch in G^{op} invers zu G. Schließlich ist die binäre Verknüpfung $*$ ist assoziativ, da

   $$g_1 * (g_2 * g_3) = g_1 * (g_3 \cdot g_2) = (g_3 \cdot g_2) \cdot g_1 = g_3 \cdot (g_2 \cdot g_1) = (g_2 \cdot g_1) * g_3 = (g_1 \cdot g_2) * g_3$$

   für alle $g_1, g_2, g_3 \in G^{\mathrm{op}}$ gilt.

2. Die Gruppen G und G^{op} haben bereits dieselbe zugrundeliegende Menge. Sie sind also gleich, wenn $\cdot = *$ gilt, wenn also $g_1 \cdot g_2 = g_1 * g_2$ für alle $g_1, g_2 \in G$ gilt. Per Definition von $*$ ist dies äquivalent dazu, dass G abelsch ist.

3. Die Abbildung $i \colon G \to G^{\mathrm{op}}$, $g \mapsto g^{-1}$ ist ein Gruppenisomorphismus, denn sie ist bijektiv mit

   $$i(g_1 \cdot g_2) = (g_1 \cdot g_2)^{-1} = g_2^{-1} \cdot g_1^{-1} = i(g_2) \cdot i(g_1) = i(g_1) * i(g_2)$$

   für alle $g_1, g_2 \in G$.

Lösung 7.

1. Für alle $h_1, h_2 \in G$ gilt

$$c_g(h_1h_2) = gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} = c_g(h_1)c_g(h_2),$$

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

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

also ist c_g bijektiv mit $c_g^{-1} = c_{g^{-1}}$.

2. Für alle $g_1, g_2 \in G$ gilt

$$c_{g_1g_2}(h) = (g_1g_2)h(g_1g_2)^{-1} = g_1g_2hg_2^{-1}g_1^{-1} = c_{g_1}(c_{g_2}(h)) \qquad \text{für alle } h \in G$$

und somit $c_{g_1g_2} = c_{g_1}c_{g_2}$.

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

Lösung 8.

1. Es sei $g \in G$. Die Konjugationsabbildung $c\colon G \to G$, $h \mapsto ghg^{-1}$ ist eine Gruppenautomorphismus. Nach Annahme gilt somit $c = \mathrm{id}_G$, weshalb $g \in \mathrm{Z}(G)$ gilt.

2. Die Invertierungsabbildung $i\colon G \to G$, $x \mapsto -x$ ist ein Gruppenhomomorphismus, da G abelsch ist. Da i bijektiv ist, handelt es sich bereits um einen Gruppenautomorphismus, weshalb nach Annahme $i = \mathrm{id}_G$ gilt. Für jedes $x \in G$ gilt somit $x = -x$, also $2x = 0$.

3. Durch $\overline{n} \cdot x = n \cdot x$ wird eine $\mathbb{F}_2$-Vektorraumstruktur auf G definiert. Da $2x = 0$ für alle $x \in G$ gilt, ist die Verknüpfung wohldefinert, und die Vektorraumaxiome ergeben sich durch direktes Nachrechnen.

4. Es sei $(b_i)_{i \in I}$ eine Basis von G als $\mathbb{F}_2$-Vektorraum. Gilt $\dim_{\mathbb{F}_2} G \geq 2$, also $|I| \geq 2$, so gibt es für eine nicht-triviale Bijektion $\sigma\colon I \to I$, die wiederum einen nicht-trivialen $\mathbb{F}_2$-Vektorraumautomorphismus $\varphi\colon G \to G$ induziert. Dann ist φ insbesondere additiv, und somit ein nicht-triviales Element von $\operatorname{Aut}(G)$.

   Es muss also $\dim_{\mathbb{F}_2} G \in \{0, 1\}$ gelten, und somit $G = 0$ oder $G \cong \mathbb{Z}/2$ als (abelsche) Gruppen. Diese beiden Gruppen erfüllen auch die gewünschte Eigenschaft.

Lösung 9.
Es sei $(a_i)_{i\in I}$ ein Repräsentantensystem der H-Linksnebenklassen in G, d.h. es sei G die disjunkte Vereinigung der Linksnebenklassen a_iH, $i \in I$. Analog sei $(b_j)_{j\in J}$ ein Repräsentantensystem der K-Linksnebenklassen in H, d.h. es sei H die disjunkte Vereinigung der Linksnebenklassen b_jK, $j \in J$.

Für jedes $i \in I$ ist die die Abbildung $H \to a_iH$, $h \mapsto a_ih$ eine Bijektion, weshalb dann auch a_iH die disjunkte Vereinigung der Linknebenklassen a_ib_jK, $j \in J$ ist. Insgesamt ist somit G disunkte Vereinigung der Linksnebenklassen a_ib_jK, $(i, j) \in I \times J$. Also ist $(a_ib_j)_{(i,j)\in I\times J}$ ein Repräsentantensystem der K-Nebenklassen in G. Somit gilt

$$[G : K] = |I \times J| = |I||J| = [G : H][H : K] .$$

Lösung 10.

- Es sei zunächst N normal in G, so dass G/N abelsch ist. Für alle $g, h \in G$ kommutieren dann $\overline{g}, \overline{h} \in G/N$, weshalb

  $$[\overline{g}, \overline{h}] = \overline{g}\overline{h}\overline{g}^{-1}\overline{h}^{-1} = \overline{ghg^{-1}h^{-1}} = \overline{[g, h]}$$

  trivial ist. Es gilt also $[g, h] \in N$ für alle $g, h \in G$, und somit

  $$[G, G] = \langle [g, h] \mid g, h \in G\rangle \subseteq N .$$

- Es gelte nun andererseits $N \subseteq [G, G]$. Die Untergruppe $[G, G] \subseteq G$ ist normal mit abelschen Quotienten $G/[G, G]$.

  Deshalb ist $N/[G, G]$ eine normale Untergruppe von $G/[G, G]$. Aus der Vorlesung ist bekannt, dass durch $K \mapsto K/[G, G] = K'$ eine 1:1-Korrespondenz zwischen den Zwischengruppen $[G, G] \subseteq K \subseteq G$ und den Untergruppen $K' \subseteq G/[G, G]$ gegeben ist, die sich auch auf die jeweils normalen Untergruppen einschränkt.

  Insbesondere ist $N/[G, G]$ normal in G, da $N/[G, G]$ normal in $G/[G, G]$ ist. Nach dem zweiten Isomorphiesatz gilt zudem, dass

  $$G/N \cong (G/[G, G])/(N/[G, G])$$

  als Quotient der abelschen Gruppe $G/[G, G]$ ebenfalls abelsch ist.

Lösung 11.

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. Da für $g \in G$ ist die Abbildung $c_g \colon G \to G$, $x \mapsto gxg^{-1}$ ein Gruppenautomorphismus ist (siehe Übung 7), ist auch $c_g(N) = gNg^{-1}$ eine Untergruppe von G von Ordnung $|N|$. Aus der Eindeutigkeit von N bezüglich dieser Eigenschaft folgt, dass bereits $gNg^{-1} = N$ gilt. Da dies für jedes $g \in G$ gilt, ist N 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 $|N|$. Wir betrachten die Ordnung $|\pi(H)|$:

   Zum einen ist $\pi(H)$ eine Untergruppe von G/N, weshalb $|\pi(H)|$ ein Teiler von $|G/N| = [G : N]$ ist. Zum anderen gilt $\ker \pi|_H = H \cap \ker \pi = H \cap N$ weshalb

   $$\pi(H) = \operatorname{im} \pi|_H \cong H/\ker \pi|_H \cong H/(H \cap N)$$

   gilt. Dabei ist $|\pi(H)| = |H/(H \cap N)| = [H : H \cap N]$ ein Teiler von $|H| = |N|$.

   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 $H = N$.

5. Ist N nicht normal in G, so kann es auch noch andere Untergruppen von Ordnung $|N|$ geben. Man betrachte etwa die symmetrische Gruppe $G = S_3$ und die Untergruppen $H_1 = \langle (1\,2) \rangle$, $H_2 = \langle (1\,3) \rangle$, $H_3 = \langle (2\,3) \rangle$ mit $|H_i| = 2$ und $[G : H_i] = 3$.

Lösung 12.
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.

Lösung 13.
Es sei $n \coloneqq [G : H]$. Die Gruppe G wirkt auf der Menge der Nebenklassen $X \coloneqq G/H$ vermöge $g.(g'H) = (gg)H$. Diese Wirkung entspricht einem Gruppenhomomorphismus $\varphi\colon G \to S(X)$ in die symmetrische Gruppe $S(X)$. Der Stabilisator des Elements $N \in X$ ist dabei genau die Untergruppe N selbst, denn für alle $g \in G$ gilt

$$g.N = N \iff gN = N \iff gN = 1N \iff 1^{-1}g \in N \iff g \in N\,.$$

Für $g \in G$ gilt genau dann $g \in \ker \varphi =: K$, wenn $g.x = x$ für alle $x \in X$ gilt, wenn also $g \in \bigcap_{x \in X} G_x$ gilt. Es gilt also $K = \bigcap_{x \in X} G_x \subseteq H$. Dabei ist K normal, da es sich um den Kern eines Gruppenhomomorphismus handelt. Außerdem hat

K endlichen Index in G, denn es gilt $G/K = G/\ker\varphi \cong \operatorname{im}\varphi \subseteq S_n$ und somit $[G : K] = |G/K| = |\operatorname{im}\varphi| \leq |S_n| = n! < \infty$. Somit lässt sich $N = K$ wählen.

Lösung 14.

1. Wir geben zwei Beweise:
   - Wir zeigen, dass $gN = Ng$ für alle $g \in G$ gilt, dass also für jedes $g \in G$ die entsprechenden Rechts- und Nebenklassen übereinstimmen. Es gibt genau zwei Linksnebenklassen, von denen eine N selbst ist; da G die disjunkte Vereinigung der beiden Nebenklassen ist, muss es sich bei der anderen Linksnebenklassen um das Komplement $G \setminus N$ handeln. Analog ergibt sich, dass N und $G \setminus N$ die beiden Rechtsnebenklassen sind. Für $g \in G$ unterscheiden wir nun zwischen zwei Fällen:
     - Gilt $g \in N$, so gilt $gN = N = Ng$.
     - Gilt $g \notin N$, so gelten $gN \neq N$ und $Ng \neq N$. Dann gelten notwendigerwiese $gN = G \setminus N = Ng$.
   - Es sei $X \coloneqq G/N$ die Menge der Linknebenklassen und $x_0 \coloneqq N \in X$. Die Gruppe G wirkt auf der Menge der Linksnebenklassen durch $g.(g'N) = (gg')N$. Es sei $\varphi\colon G \to S(X)$ der entsprechende Gruppenhomomorphismus in die symmetrische Gruppe der Menge X. Für $g \in G$ gilt genau dann $g \in \ker\varphi$, wenn $g.x = x$ für alle $x \in X$ gilt, d.h. wenn g jedes Element aus X fixiert. Da X nach Annahme zweielementig ist, ist dies äquivalent dazu, dass g das Element x_0 fixiert, also $gN = N$ gilt. Dies genau für $g \in N$. Also gilt $\ker\varphi = N$, weshalb N normal in G ist.

2. Wir geben zwei Arten von Gegenbeispielen an:
   - Es sei $G \coloneqq S_p$ die symmetrische Gruppe und $H \coloneqq \{\sigma \in S_p \mid \sigma(1) = 1\}$. Es gilt $H \cong S_{p-1}$ und somit $[G : H] = |G|/|H| = p!/(p-1)! = p$. Die Untergruppe H ist allerdings nicht normal in G, denn für den Zykel $\sigma = (2\ 3\ \cdots\ p) \in H$ und die Transposition $\tau = (1\ 2)$ gelten
   $$(\tau\sigma\tau^{-1})(1) = (\tau\sigma\tau)(1) = \tau(\sigma(\tau(1))) = \tau(\sigma(2)) = \tau(3) = 3\,,$$
   und deshalb $\tau\rho\tau^{-1} \notin H$.
   - Es sei $G \coloneqq D_p$ die Diedergruppe von Ordnung $2p$ und $\tau \in D_p$ eine Spiegelung. Dann ist $H \coloneqq \langle\tau\rangle = \{1, \tau\}$ eine Untergruppe vom Index p. Ist aber $\rho \in D_p$ eine Rotation um den Winkel $2\pi/p$, so gilt $\tau\rho\tau = \rho^{-1} \neq \rho$, weshalb τ und ρ nicht kommutieren. Dann gilt auch $\rho\tau\rho^{-1} \neq \tau$, und somit $\rho H\rho^{-1} \neq H$.

Lösung 15.

1. Für jedes $g \in G$ ist die Konjugationsabbildung $c\colon G \to G$, $h \mapsto ghg^{-1}$ ein Automorphismus. Da N charakteristisch ist, gilt deshalb $gNg^{-1} = c(N) = N$.

2. Ist $\varphi\colon G \to G'$ ein Isomorphismus von Gruppen, so gilt $\varphi(\mathrm{Z}(G)) = \mathrm{Z}(G')$. Insbesondere gilt für jeden Automorphismus $\varphi \in G \to G$, dass $\varphi(\mathrm{Z}(G)) = \mathrm{Z}(\varphi(G)) = \mathrm{Z}(G)$.

Für jeden Gruppenhomomorphismus $\varphi\colon G \to G'$ gilt $\varphi([G,G]) = [\varphi(G), \varphi(G')]$. Inbesondere gilt $\varphi([G,G]) = [\varphi(G), \varphi(G)] = [G,G]$ für jeden Automorphismus $\varphi\colon G \to G$.

3. Es sei $g \in G$ und $c\colon G \to G$, $h \mapsto ghg^{-1}$ die Konjugationsabbildung. Da N normal ist, schränkt sich der Automorphismus c_g zu einem Automorphismus $c_g|_N\colon N \to N$ ein (das Inverse ist durch die Einschränkung der Konjugation mit g^{-1} gegeben). Da K charakteristisch in N ist, gilt $gKg^{-1} = c_g(K) = c_g|_N(K) = K$.

4. Also ist $\mathrm{Z}(N)$ eine charakteristische Untergruppe von N. Da N normal ist in G ist folgt deshalb auch dem vorherigen Aufgabenteil, dass auch $\mathrm{Z}(N)$ auch normal in G.

Lösung 16.

1. Für jedes $g \in G$ gilt $g^{-1} = g$, und für alle $g, h \in G$ gilt somit
$$gh = g^{-1}h^{-1} = (hg)^{-1} = hg\,.$$

2. Die Gruppe
$$G = \left\{ \begin{pmatrix} 1 & * & \cdots & * \\ & \ddots & \ddots & \vdots \\ & & \ddots & * \\ & & & 1 \end{pmatrix} \right\} \subseteq \mathrm{GL}_p(\mathbb{F}_p)$$
ist nicht abelsch. Es gilt aber $A^p = I$ für jede Matrix $A \in G$, denn das charakteristische Polynom von A ist $\chi_A(t) = (t-1)^p = t^p - 1$, und nach dem Satz von Cayley–Hamilton gilt deshalb $0 = \chi_A(A) = A^p - I$.

Lösung 17.

1. Es sei $\overline{g} \in G/\mathrm{Z}(G)$ ein zyklischer Erzeuger. Für alle $x, y \in G$ gibt es dann $n, m \in \mathbb{Z}$ mit $\overline{x} = \overline{g}^m = \overline{g^m}$ und $y = \overline{g}^n = \overline{g^n}$. Es gibt dann $x', y' \in \mathrm{Z}(G)$ mit $x = g^m x'$ und $y = g^n y'$. Die Element x', y', g^n, g^m kommutieren paarweise miteinander, weshalb auch x und y kommutieren.

2. Da G nicht abelsch ist, kann $G/\mathrm{Z}(G)$ nach dem vorherigen Aufgabenteil nicht zyklisch sein. Deshalb muss $[G : \mathrm{Z}(G)] \geq 4$ gelten (denn Gruppen der Ordnung < 4 sind stets zyklisch). Es gilt also $|\mathrm{Z}(G)| \leq |G|/4$, bzw. $|G \smallsetminus \mathrm{Z}(G)| \geq (3/4)|G|$.

3. Es gilt $1x = x = x1$ und somit $1 \in Z_G(x)$. Für alle $y, z \in x$ gilt $yzx = yxz = xyz$ und somit auch $yz \in Z_G(x)$. Für jedes $y \in Z_G(x)$ gilt außerdem
$$y^{-1}x = y^{-1}xyy^{-1} = y^{-1}yxy^{-1} = xy^{-1}$$
und somit auch $y^{-1} \in Z_G(x)$. Dies zeigt, dass $Z_G(x)$ eine Untergruppe von G ist.

   Ist x nicht zentral, so ist $Z_G(x)$ bereits eine echte Untergruppe von G. Dann gilt $[G : Z_G(x)] \geq 2$ und somit $|Z_G(x)| \leq |G|/2$, bzw. $|G \smallsetminus Z_G(x)| \geq |G|/2$.

4. Da G nicht abelsch ist, sind mindestens $3/4$ aller Gruppenelemente $x \in G$ nicht zentral. Für jedes solche x kommutiert das Paar (x, y) dann für mindestens die Hälfte aller $y \in G$ nicht. Insgesamt ergeben sich somit mindestens $(3/4)\cdot(1/2) = 3/8$ nicht kommutierende Paare.

Lösung 18.

1. Es sind $G.x = \{g.x \mid g \in G\}$ und $G_x = \{g \in G \mid g.x = x\}$.

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 $gG_y g^{-1} = G_x$ gilt.

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 $x = g.y$; 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 $x \sim z$.

Lösung 19.
Es sei $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ der Normalisator der Untergruppe H. Die Anzahl der Konjugate der Untergruppe H ist durch den Index $[G : N_G(H)]$ gegeben:

Die Gruppe G wirkt auf der Menge $\mathcal{S}$ der Untergruppen von G durch Konjugation. Die Bahn $G.H$ der Untergruppe $H \in \mathcal{S}$ sind genau die Menge der Konjugate $\{gHg^{-1} \mid g \in G\}$, und der Stabilisator G_H der Untergruppe $H \in \mathcal{S}$ ist genau der Normalisator $N_G(H)$. Durch die induzierte Bijektion

$$G/N_G(H) = G/G_H \to G.H = \{gHg^{-1} \mid g \in G\}\,, \quad gN_G(H) \mapsto g.H = gHg^{-1}$$

ergibt sich mit $|G/N_G(H)| = [G : N_G(H)]$ die gewünschte Gleichheit.

Es seien $n \coloneqq [G : N_G(H)]$ und $g_1Hg_1^{-1}, \ldots, g_nHg_n^{-1}$ die paarweise verschiedenen Konjugate von H. Dabei gilt $n = [G : N_G(H)] \leq [G : H]$, da $H \subseteq N_G(H)$ eine Untergruppe ist. Außerdem sind die Konjugate $g_iHg_i^{-1}$ jeweils Untergruppen von G, und enthalten somit alle das neutrale Element $1 \in G$. Damit ergibt sich, dass

$$\begin{aligned}\left|\bigcup_{g\in G} gHg^{-1}\right| = \left|\bigcup_{i=1}^{n} g_iHg_i^{-1}\right| &\leq [G : N_G(H)] \cdot |H| - (n-1) \\ &\leq [G : H] \cdot |H| - (n-1) = |G| + (1-n)\,.\end{aligned}$$

Die Gleichheit $G = \bigcup_{g\in G} gHg^{-1}$ kann deshalb nur für $n = 1$ gelten. Dann wäre aber bereits $G = g_1Hg_1^{-1}$, also $|G| = |g_1Hg_1^{-1}| = |H|$, und somit H keine echte Untergruppe von G.

Lösung 20.

1. Es seien $x_1, \ldots, x_n \in X$ Repräsentanten der nicht-trivalen Bahnen. Nach der Bahnenformel gilt dann

$$|X| = |X^G| + \sum_{i=1}^{n} |G.x_i| = |X^G| + \sum_{i=1}^{n} [G : G_{x_i}]\,.$$

Da die G-Mengen $G.x_i$ nicht trivial sind, gilt dabei $|G.x_i| = [G : G_{x_i}] \neq 1$, wobei $[G : G_{x_i}]$ ein Teiler der Gruppenordnung $|G|$ ist. Es ist also $[G : G_{x_i}]$ jeweils eine nicht-triviale p-Potzenz, und somit $[G : G_{x_i}] \equiv 0 \pmod p$. Somit gilt insgesamt

$$|X| = |X^G| + \sum_{i=1}^{n} [G : G_{x_i}] \equiv |X^G| + 0 = |X^G| \pmod p\,.$$

Gilt $p \nmid |X|$, so folgt aus $|X^G| \equiv |X| \not\equiv 0 \pmod p$, dass $|X^G| \neq 0$, also $X^G \neq \emptyset$.

2. a) Die Gruppe G wirke auf sich selbst, also auf $X = G$, durch Konjugation. Dann gilt $X^G = \mathrm{Z}(G)$ und somit nach dem ersten Aufgabenteil

$$|\mathrm{Z}(G)| = |X^G| = |X| = |G| \equiv 0\,.$$

Also ist $|\mathrm{Z}(G)|$ ein Vielfaches von p. Der Fall $|\mathrm{Z}(G)| = 0$ kann dabei nicht eintreten, da $\mathrm{Z}(G)$ als Untergruppe nicht leer ist. Folglich gilt $|\mathrm{Z}(G)| \geq p$, weshalb $\mathrm{Z}(G)$ nicht trivial ist.

b) Da N normal in G ist, wirkt G durch Konjugation auf $Y = N$. Ersetzt man nun in der obigen Argumentation X durch Y und X^G durch $Y^G = N \cap \mathrm{Z}(G)$, so ergibt sich, dass $N \cap \mathrm{Z}(G)$ nicht trivial ist.

3. Es sei $\mathcal{S}$ die Menge der Untergruppen von G. Die Gruppe G wirkt auf der Menge $\mathcal{S}$ durch Konjugation, d.h. vermöge $g.H = gHg^{-1}$ für alle $g \in G$, $H \in \mathcal{S}$. Eine Untergruppe $N \in \mathcal{S}$ ist genau dann normal in G, wenn N ein Fixpunkt dieser Wirkung ist. Es gilt also zu zeigen, dass $|\mathcal{S}| - |\mathcal{S}^G|$ ein Vielfaches von p ist, dass also $|\mathcal{S}| \equiv |\mathcal{S}^G| \pmod{p}$ gilt. Dies ergibt sich aus dem vorherigen Aufgabenteil.

Lösung 21.

1. Jede p-Untergruppe von H ist auch eine p-Untergruppe von G. Da P eine maximale p-Untergruppe von G ist, handelt es sich deshalb auch um eine maximale p-Untergruppe von G.

2. Die Gruppe H ist eine p-Untergruppe von G. Somit gibt es eine p-Sylowuntergruppe P' von G mit $P \subseteq P'$. Dann ist $H \cap P'$ eine Untergruppe von H mit $P \subseteq H \cap P'$. Dabei ist $H \cap P'$ eine p-Gruppe, da P' eine p-Gruppe ist. Da P maximal unter allen p-Untergruppen von H ist, gilt bereits $P = H \cap P'$.

3. Es sei P' eine p-Sylowuntergruppe von G mit $P = H \cap P'$. Die normale p-Sylowuntergruppe von G ist bereits die eindeutige p-Sylowuntergruppe von G (denn alle p-Sylowuntergruppen von G sind konjugiert zueinander). Also ist P' bereits diese eindeutige p-Sylowuntergruppe von G. Inbesondere ist $P = H \cap P'$ bereits eindeutig bestimmt. Also ist P die eindeutige p-Sylowuntergruppe von H. Damit ist P normal in H (denn alle H-Konjugierten von P sind ebenfalls p-Sylowuntergruppen von H).

4. Es sei P' eine p-Sylowuntergruppe. Dann gibt es eine p-Sylowuntergruppe P'' von G mit $P' = H \cap P''$. Die beiden p-Sylowuntergruppen P und P'' von G sind konjugiert zueinander, weshalb es ein Gruppenelement $g \in G$ mit $gPg^{-1} = P''$ gibt. Dann gilt

$$g(H \cap P)g^{-1} = (gHg^{-1}) \cap (gPg^{-1}) = H \cap P'' = P' .$$

   Inbesondere gilt somit $|H \cap P| = |P'|$, weshalb auch $H \cap P$ eine maximale p-Untergruppe von H ist, und somit eine p-Sylowuntergruppe von H.

5. Es gilt $P, P' \subseteq N_G(P)$. Nach dem ersten Aufgabenteil sind P und P' bereits p-Sylowuntergruppen von $N_G(P)$. Da P normal in $N_G(P)$ ist, besitzt $N_G(P)$ allerdings eine eindeutige p-Sylowuntergruppe (denn alle anderen p-Sylowuntergruppen von $N_G(P)$ sind in $N_G(P)$ konjugiert zu P). Folglich muss bereits $P = P'$ gelten.

6. Die Inklusion $K \subseteq N_G(K)$ gilt für jede Untergruppe $K \subseteq G$, also insbesondere für $K = H$.

   Andererseits sei $a \in N_G(H)$. Nach dem ersten Aufgabenteil ist P eine p-Sylowuntergruppe von H, weshalb aPa^{-1} eine P-Sylowuntergruppe von $aHa^{-1} = H$ ist.

Die p-Sylowuntergruppen P und aPa^{-1} von H sind in H konjugiert zueinander, weshalb es ein Gruppenelement $b \in H$ mit

$$P = baPa^{-1}b^{-1} = (ba)P(ba)^{-1}$$

gibt. Dann ist $ba \in N_G(P) \subseteq H$ und wegen $b \in H$ somit auch $a = b^{-1}ba \in H$.

Mit $H = N_G(P)$ ergibt sich, dass $N_G(N_G(P)) = N_G(P)$.

Lösung 22.

Ist $\mathcal{O} \in X/G$ eine G-Bahn und $x \in X$ mit $\mathcal{O} = G.x$, so ist $|\mathcal{O}| = |G.x| = [G : G_x]$ ein Teiler von $|G|$. Für die Ordnung von G gilt $|G| = 77 = 7 \cdot 11$, also gilt $|\mathcal{O}| \in \{1, 7, 11, 77\}$ für jede G-Bahn $\mathcal{O} \in X/G$. Dabei gilt genau dann $|\mathcal{O}| = 1$, falls $\mathcal{O} = \{x\}$ 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 $17 = |X| = \sum_{\mathcal{O} \in X/G} |\mathcal{O}|$. 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.

Lösung 23.

Für jedes $x \in X$ sei $\mathcal{O}_x \coloneqq \{g.x \mid g \in G\}$ die Bahn von x. Wegen der Bijektion $G/G_x \to \mathcal{O}_x$, $gG_x \mapsto g.x$ gilt $|\mathcal{O}_x| = |G/G_x| = |G|/|G_x|$. Für alle $g \in G$, $x \in X$ gilt

$$g \in G_x \iff g.x = x \iff x \in \mathrm{Fix}(g)\,.$$

Deshalb gilt

$$\sum_{g \in G} |\mathrm{Fix}(g)| = \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|\mathcal{O}_x|} = |G| \sum_{x \in X} \frac{1}{|\mathcal{O}_x|}\,.$$

Hieraus folgt, dass

$$\frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)| = \sum_{x \in X} \frac{1}{|\mathcal{O}_x|} = \sum_{\mathcal{O} \in X/G} \sum_{x \in \mathcal{O}} \frac{1}{|\mathcal{O}|} = \sum_{\mathcal{O} \in X/G} 1 = |X/G|\,.$$

Lösung 24.

1. Aufgrund der Bijektion $G/G_x \to G.x$, $gG_x \mapsto g.x$ gilt $|G.x| = |G/G_x| = |G|/|G_x|$.
2. Die Gruppe G wirke auf sich selbst vermöge Konjugation, d.h. für alle $g \in G$, $x \in G$ gelte $g.x \coloneqq gxg^{-1}$. Die Konjugationsklassen von G sind genau die Bahnen dieser Gruppenwirkung. Nach dem vorherigen Aufgabenteil ist somit die Kardinalität jeder Konjugationsteiler ein Teiler der Gruppenordnung $|G|$.

Die Konjugationsklasse des neutralen Elements $e \in G$ ist stets die einelementige Menge $\{e\}$. Da G die disjunkte Vereinigung beider Konjugationsklassen ist, muss es sich bei der anderen Konjugationsklasse um $G \smallsetminus \{e\}$ handeln. Dann ist $|G \smallsetminus \{e\}| = |G| - 1$ ein Teiler von $|G|$. Dies ist nur für $|G| = 2$ möglich, wenn also $G \cong \mathbb{Z}/2$ gilt.

Lösung 25.
Für $n = 1$ ist die Gruppe $\mathrm{GL}_n(K) = \mathrm{GL}_1(K) \cong K^\times$ abelsch. Für $n \geq 2$ ist die Gruppe $\mathrm{GL}_n(K)$ nie abelsch: Für $n = 2$ gibt es das Gegenbeispiel

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

und für alle $n \geq 2$ ergibt sich hieraus, dass $ST \neq TS$ für die beiden Matrizen $S, T \in \mathrm{GL}_n(K)$ mit

$$S = \begin{pmatrix} 0 & 1 & & & \\ 1 & 0 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 & & & \\ 0 & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}.$$

Lösung 26.
Die Gruppen S_1 und S_2 sind abelsch, weshalb $\mathrm{Z}(S_1) = S_1$ und $\mathrm{Z}(S_2) = S_2$ gelten. Für alle $n \geq 3$ gilt $\mathrm{Z}(S_n) = 1$: Für jedes $\sigma \in \mathrm{Z}(S_n)$ sei

$$F_\sigma = \{i \in \{1, \ldots, n\} \mid \sigma(i) = i\}$$

die Fixpunktmenge von σ. Für jedes $i \in F_\sigma$ gilt auch $\pi(i) \in F_\sigma$, denn

$$\sigma(\pi(i)) = \pi(\sigma(i)) = \pi(i).$$

Da $n \geq 3$ gilt, gibt es für jedes $i \in \{1, \ldots, n\}$ eine Permutation $\sigma \in S_n$ mit $F_\sigma = \{i\}$, etwa den Zykel $\sigma \coloneqq (1\,2\,\cdots\,i\,(i+2)\,\cdots\,n)$. Dann gilt $\{\pi(i)\} = \pi(\{i\}) = \{i\}$ und somit $\pi(i)$. Also gilt $\pi(i) = i$ für alle $i \in \{1, \ldots, n\}$, und somit $\pi = \mathrm{id}$.

Lösung 27.
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 $h_2 \notin H_1$. 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 $h_1 h_2 \notin H_1$ 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 Aussagenteil 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 $H_i \nsubseteq H_j$ für alle $1 \leq i \neq j \leq 3$, aber $H_1 \cup H_2 \cup H_3 = G$.

Lösung 28.

1. Für jede Gruppe H notieren wir die iterierten Kommutatoren mit $D^1(H) \coloneqq H$ und $D^{i+1} \coloneqq [D^i(H), D^i(H)]$.

   Es gilt $D^1(H) = H \subseteq G = D^1(G)$ und somit induktiv $D^i(H) \subseteq D^i(G)$ für alle $i \geq 1$.

   Für die kanonische Projektion $\pi \colon G \to G/N$ gilt

$$\pi(D^1(G)) = \pi(G) = G/N = D^1(G/N)\,.$$

   Gilt $\pi(D^i(G)) = D^i(G/N)$ für ein $i \geq 1$, so gilt auch

$$\begin{aligned} \pi(D^{i+1}(G)) = \pi([D^i(G), D^i(G)]) &= [\pi(D^i(G)), \pi(D^i(G))] \\ &= [D^i(G/N), D^i(G/N)] = D^{i+1}(G/N)\,. \end{aligned}$$

   Induktiv ergibt sich also, dass $\pi(D^i(G)) = D^i(G/N)$ für alle $i \geq 1$ gilt.

   Es sei nun G auflösbar, d.h. es gebe $n \geq 1$ mit $D^n(G) = 1$. Dann gilt auch $D^n(N) \subseteq D^n(G) = 1$, also $D^n(N) = 1$, weshalb N auflösbar ist. Es gilt auch $D^n(G/N) = \pi(D^n(G)) = \pi(1) = 1$, weshalb G/N auflösbar ist.

   Es seien nun die Gruppen N und G/N beide auflösbar. Dann gibt es $n, m \geq 1$ mit $D^n(N) = 1$ und $D^m(G/N) = 1$. Dann gilt $\pi(D^m(G)) = D^m(G/N) = 1$ und somit $D^m(G) \subseteq \ker \pi = N$. Damit gilt ferner $D^{n+m}(G) = D^n(D^m(G)) \subseteq D^n(N) = 1$, also $D^{n+m}(G) = 1$. Also ist G auflösbar.

2. Es sei G eine Gruppe der Ordnung pq wobei o.B.d.A. $p < q$ gelte. Bezeichnet n_q die Anzahl der q-Sylowuntergruppen von G, so gilt $n_q \mid p$ und $n_q \equiv 1 \pmod{p}$. Also muss $n_q = 1$ gelten. Die somit eindeutige q-Sylowuntergruppe N von G ist normal in G (denn die Konjugate von N sind ebenfalls q-Sylowuntergruppen von G). Es gilt $|N| = q$, also $N \cong \mathbb{Z}/q$, weshalb N abelsch und somit auflösbar ist. Es gilt auch $|G/N| = p$, also $G/N \cong \mathbb{Z}/p$, weshalb G/N abelsch und somit auflösbar ist. Da N und G/N beide auflösbar sind, ist auch G auflösbar.

3. Die Primfaktoren von 30 sind $2, 3, 5$. Für jeden Primfaktor $p \in \{2, 3, 5\}$ sei n_p die Anzahl der p-Sylowuntergruppen von G. Es gelten $n_3 \mid 10$ und $n_3 \equiv 1 \pmod 3$ und somit $n_3 \in \{1, 10\}$. Analog ergibt sich, dass $n_5 \in \{1, 6\}$.

   Wären $n_3 = 10$ und $n_5 = 6$, so gäbe es in G mindestens 20 Elemente der Ordnung 3 und 25 Elemente der Ordnung 5 (denn jede 3-Sylowuntergruppe von G ist isomorph zu $\mathbb{Z}/3$, und jede 5-Sylowuntergruppe von G ist isomorph zu $\mathbb{Z}/5$). Dann wäre aber $30 = |G| \leq 20 + 25 = 45$.

   Es gilt also $n_3 = 1$ oder $n_5 = 1$. Gilt $n_3 = 1$, so besitzt G eine 3-Sylowuntergruppe N. Dann gilt $|N| = 3$, also $N \cong \mathbb{Z}/3$, weshalb N abelsch und somit auflösbar sind. Außerdem gilt dann $|G/N| = 10 = 2 \cdot 5$, weshalb G/N nach dem vorherigen Aufgabenteil ebenfalls auflösbar ist. Dann sind N und G/N auflösbar, weshalb dann auch G auflösbar ist. Analog ergibt sich die Auflösbarkeit von G im Fall $n_5 = 1$.

Lösung 29.

1. Die kanonischen Projektionen $\pi_i \colon G_i \to G_i/N_i$, $g \mapsto \overline{g}$ induzieren einen Gruppenhomomorphismus

$$\pi \coloneqq \pi_1 \times \pi_2 \colon G_1 \times G_2 \to (G_1/N_1) \times (G_2/N_2), \quad (g_1, g_2) \mapsto (\overline{g_1}, \overline{g_2}).$$

   Da π_1 und π_2 surjektiv sind, ist es auch π. Außerdem gilt

$$\ker \pi = \ker \pi_1 \times \ker \pi_2 = N_1 \times N_2$$

   Somit ist $N_1 \times N_2$ eine normale Untergruppe von $G_1 \times G_2$, und π induziert einen Isomorphismus

$$\overline{\pi} \colon (G_1 \times G_2)/(N_1 \times N_2) \to (G_1/N_1) \times (G_2/N_2), \quad \overline{(g_1, g_2)} \mapsto (\overline{g_1}, \overline{g_2}).$$

2. Da G_1 auflösbar ist gibt es eine Kette von Untergruppen

$$1 = N_0 \subseteq N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots \subseteq N_{s-1} \subseteq N_s = G_1,$$

   so dass für alle $i = 1, \ldots, s$ die Untergruppe N_{i-1} normal in N_i ist, und der Quotient N_i/N_{i-1} abelsch ist. Aus der Auflösbarkeit von G_2 ergibt sich analog eine Kette von Untergruppen

$$1 = K_0 \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq \cdots \subseteq K_{t-1} \subseteq K_t = G_1,$$

   so dass für alle $j = 1, \ldots, t$ die Untergruppe K_{j-1} normal in K_j ist, und der Quotient K_j/K_{j-1} abelsch ist. Zusammen erhalten wir damit eine Kette von Untergruppen

$$1 \times 1 = N_0 \times 1 \subseteq \cdots \subseteq N_s \times 1 = G_1 \times K_0 \subseteq \cdots \subseteq G_1 \times K_t = G_1 \times G_2.$$

Nach dem vorherigen Aussagenteil ist in dieser Kette jede Untergruppe normal in der jeweils nächsten Untergruppe. Die Quotienten sind abelsch, denn für alle $i = 1, \ldots, s$ gilt

$$(N_i \times 1)/(N_{i-1} \times 1) \cong (N_i/N_{i-1}) \times (1/1) \cong (N_i/N_{i-1}) \times 1 \cong N_i/N_{i-1}$$

und für alle $j = 1, \ldots, t$ gilt

$$(G_1 \times K_j)/(G_1 \times K_{j-1}) \cong (G_1/G_1) \times (K_j/K_{j-1}) \cong 1 \times (K_j/K_{j-1}) \cong K_i/K_{j-1}.$$

Lösung 30.

Im Folgenden sind alle auftretenden Gruppen abelsch. Insbesondere sind jeweils alle betrachteten Untergruppen normal, weshalb sich jeweils die entsprechenden Quotientengruppen bilden lassen.

1. Für $|G| = p^n$ zeigen wir die Aussage per Induktion über $n \geq 1$.

   Für $n = 1$ gilt $|G| = p$ und es lässt sich $H = 0$ wählen.

   Gilt $n \geq 2$, so gibt es ein Element $g \in G$ mit $g \neq 0$. Dann ist $\langle g \rangle \subseteq G$ eine nichttriviale Untergruppe. Es sei $\pi \colon G \to G/\langle g \rangle$ die kanonische Projektion. Es ist $G/\langle g \rangle$ eine p-Gruppe von Ordnung $|G/\langle g \rangle| < |G|$, weshalb es nach Induktionsvoraussetzung eine Untergruppe $H' \subseteq G/\langle g \rangle$ vom Index p gibt.

   Aus der Vorlesung ist bekannt, dass durch $K \mapsto K'/\langle g \rangle$ eine 1:1-Korrespondenz zwischen den Zwischengruppen $\langle g \rangle \subseteq K \subseteq G$ und Untergruppen $K' \subseteq G/\langle g \rangle$ gegeben ist.

   Es gibt deshalb eine Untergruppe $H \subseteq G$ mit $H' = H/\langle g \rangle$. Dann gilt

   $$[G : H] = \frac{|G|}{|H|} = \frac{|G|/|\langle g \rangle|}{|H|/|\langle g \rangle|} = \frac{|G/\langle g \rangle|}{|H/\langle g \rangle|} = \frac{|G/\langle g \rangle|}{H'} = [G/\langle g \rangle : H'] = p\,,$$

   so dass H eine Untergruppe von Index p in G ist.

2. Für $|G| = p^n$ zeigen wir die Aussage per Induktion über $n \geq 0$:

   Für $n = 0$ ist nichts zu zeigen. Für $n \geq 1$ gibt es nach dem vorherigen Aufgabenteil eine Untergruppe $G_{n-1} \subseteq G$ vom Index $[G : G_{n-1}] = p$. Es gilt dann $|G/G_{n-1}| = p$ und somit $G/G_{n-1} \cong \mathbb{Z}/p$. Nach Induktionsvoraussetzung gibt es eine Normalenreihe

   $$0 = G_0 \subsetneq G_1 \subsetneq G_2 \subsetneq \cdots \subsetneq G_{n-1}$$

   mit Faktoren $G_i/G_{i-1} \cong \mathbb{Z}/p$. Ingesamt ergibt sich damit die gewünschte Normalenreihe.

Lösung 31.

1. Im Fall $p = 2$ ist der Frobeniushomomorphismus $\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $x \mapsto x^2$ ein Körperautomorphismus, weshalb dann $\mathrm{Quad}(2, n) = \mathbb{F}_{p^n}$ gilt. Inbesondere gilt dann $|\mathrm{Quad}(2, n)| = |\mathbb{F}_{2^n}| = 2^n$.

   Im Fall $p \neq 2$ gilt

   $$\mathrm{Quad}(p, n) = \{x^2 \mid x \in \mathbb{F}_{p^n}\} = \{0\} \cup \{x^2 \mid x \in \mathbb{F}_{p^n}^\times\} = \{0\} \cup \operatorname{im} q$$

   für den Gruppenhomomorphismus $q \colon \mathbb{F}_{p^n}^\times \to \mathbb{F}_{p^n}^\times$, $x \mapsto x^2$. Es gilt

   $$\ker q = \{x \in \mathbb{F}_{p^n}^\times \mid x^2 = 1\} = \{1, -1\}$$

und somit $|\ker q| = 2$ (hier nutzen wir, dass $\operatorname{char} \mathbb{F}_{p^n} = p \neq 2$ und somit $1 \neq -1$). Deshalb gilt $|\operatorname{im} q| = [\mathbb{F}_{p^n}^\times : \ker q] = |\mathbb{F}_{p^n}^\times| / |\ker q| = (p^n - 1)/2$. Ingesamt gilt somit, dass

$$|\mathrm{Quad}(p,n)| = \begin{cases} 2^n & \text{falls } p = 2, \\ \frac{p^n-1}{2} + 1 & \text{falls } p \neq 2. \end{cases}$$

2. Im Falle $p = 2$ gilt, wie bereits zuvor gesehen, dass $\mathrm{Quad}(2,n) = \mathbb{F}_{2^n}$, weshalb es sich um eine Untergruppe handelt. Im Falle $p \neq 2$ gilt $(p^n - 1)/2 + 1 \nmid p^n$, denn sonst würde

$$\begin{aligned} &\frac{p^n-1}{2} + 1 \,\Big|\, p^n \iff \frac{p^n-1}{2} + 1 \equiv 0 \pmod{p^n} \\ \iff &\frac{p^n-1}{2} \equiv -1 \pmod{p^n} \iff p^n - 1 \equiv -2 \pmod{p^n} \\ \iff &-1 \equiv -2 \pmod{p^n} \iff 1 \equiv 0 \pmod{p^n} \iff p^n \mid 1 \end{aligned}$$

gelten. Somit ist $|\mathrm{Quad}(p,n)|$ in diesem Fall kein Teiler von $|\mathbb{F}_{p^n}|$, und deshalb $\mathrm{Quad}(p,n)$ keine Untergruppe der additiven Gruppe von $\mathbb{F}_{p^n}$.

3. Für $x, y \notin \mathrm{Quad}(p,n)$ gelten inbesondere $x, y \neq 0$ und somit $x, y \in \mathbb{F}_{p^n}^\times$. Die Gruppe $\mathbb{F}_{p^n}^\times$ zyklisch, da $\mathbb{F}_{p^n}$ ein endlicher Körper ist; es sei $g \in \mathbb{F}_{p^n}^\times$ ein Erzeuger. Dann gibt es $a, b \in \mathbb{N}$ mit $x = g^a$ und $y = g^b$; da x und y keine Quadrate sind, müssen a and b ungerade sein (denn sonst wäre beispielsweise $x = g^a = (g^{a/2})^2$). Dann ist $a + b$ gerade und somit $xy = g^a g^b = g^{a+b} = (g^{(a+b)/2})^2$ ein Quadrat.

Lösung 32.

Wären die beiden Gruppen isomorph, so gäbe es genau so viele Elemente $x \in K$ mit $2x = 0$ wie Elemente $y \in K^\times$ mit $y^2 = 1$. Wir unterscheiden zwischen zwei Fällen:

- Im Fall $\operatorname{char} K = 2$ gilt $2x = 0$ für alle $x \in K$, aber das einzige Element $y \in K^\times$ mit $y^2 = 1$ ist 1.
- Im Fall $\operatorname{char} K \neq 2$ gibt es nur ein Element $x \in K$ mit $2x \neq 0$, aber es gibt zwei Elemente $y \in K^\times$ mit $y^2 = 1$ (nämlich 1 und -1).

Lösung 33.

1. Es sei $(V_1, \ldots, V_n) \in \mathcal{F}(n, K)$.

   Für jede Matrix $A \in \mathrm{GL}_n(K) = G$ sind dann $AV_1, \ldots, AV_n$ Untervektorräume von V. Wegen der Invertierbarkeit der Matrix A folgt dabei aus $V_1 \neq 0$ und $V_n = K^n$, dass $AV_1 \neq 0$ und $AV_n = K^n$, und aus $V_i \subseteq V_{i+1}$ folgt $AV_i \subsetneq AV_{i+1}$. Somit ist $A.(V_1, \ldots, V_n)$ eine Flagge in K^n.

   Für die Identitätsmatrix $I \in \mathrm{GL}_n(K)$ gilt

$$I.(V_1, \ldots, V_n) = (IV_1, \ldots, IV_n) = (V_1, \ldots, V_n)\,.$$

Für alle $A, B \in \mathrm{GL}_n(K)$ gilt

$$\begin{aligned} A.(B.(V_1, \ldots, V_n)) &= A.(BV_1, \ldots, BV_n) \\ &= (ABV_1, \ldots, ABV_n) = (AB).(V_1, \ldots, V_n)\,. \end{aligned}$$

2. Es genügt zu zeigen, dass die Bahn der Standardflagge S bereits ganz $\mathcal{F}(n, K)$ ist. Hierfür sei $(V_1, \ldots, V_n) \in \mathcal{F}(n, K)$ und $(b_1, \ldots, b_n)$ eine Basis von K^n mit $V_i = \langle b_1, \ldots, b_i \rangle$ für alle i. Die Matrix A mit Spalten $b_1, \ldots, b_n$ ist dann invertierbar, also ein Element der Gruppe $\mathrm{GL}_n(K)$, und es gilt

$$\begin{aligned} A.S &= A.(\langle e_1 \rangle, \langle e_1, e_2 \rangle, \ldots, \langle e_1, \ldots, e_n \rangle) \\ &= (A\langle e_1 \rangle, A\langle e_1, e_2 \rangle, \ldots, A\langle e_1, \ldots, e_n \rangle) \\ &= (\langle Ae_1 \rangle, \langle Ae_1, Ae_2 \rangle, \ldots, \langle Ae_1, \ldots, Ae_n \rangle) \\ &= (\langle b_1 \rangle, \langle b_1, b_2 \rangle, \ldots, \langle b_1, \ldots, b_n \rangle) = (V_1, \ldots, V_n)\,. \end{aligned}$$

3. Für $A \in \mathrm{GL}_n(K)$ gilt genau dann $A.S = S$, wenn

$$\langle Ae_1, \ldots, Ae_i \rangle = A.\langle e_1, \ldots, e_i \rangle = \langle e_1, \ldots, e_i \rangle$$

für alle $i = 1, \ldots, n$ gilt.

Dabei ist für jedes $i = 1, \ldots, n$ die Gleichheit $\langle Ae_1, \ldots, Ae_i \rangle = \langle e_1, \ldots, e_i \rangle$ wegen der Invertierbarkeit von A (und daraus folgenden linearen Unabhängigkeit von $Ae_1, \ldots, Ae_i$) äquivalent zu der Inklusion $\langle Ae_1, \ldots, Ae_i \rangle \subseteq \langle e_1, \ldots, e_i \rangle$. Diese gilt genau dann, wenn $Ae_1, \ldots, Ae_i \in \langle e_1, \ldots, e_i \rangle$ gilt, wenn also die ersten i Spalten von A nur in den ersten i Zeilen Einträgen haben.

Dass dies für alle i gilt, ist also äquivalent dazu, dass für alle $j = 1, \ldots, n$ in der j-ten Spalte von A nur Einträge in den ersten j Zeilen stehen. Dies bedeutet gerade, dass A eine obere Dreiecksmatrix ist.

4. Unter der Wirkung $\mathrm{GL}_n(\mathbb{F}_q)$ auf $\mathcal{F}(n, \mathbb{F}_q)$ die Bahn von S und $\mathrm{B}_n(\mathbb{F}_q)$ der Stabilisator von S. Also erhalten wir eine Bijektion (bzw. Isomorphismus von Links-$\mathrm{GL}_n(\mathbb{F}_q)$-Mengen)

$$\mathrm{GL}_n(\mathbb{F}_q)/\,\mathrm{B}_n(\mathbb{F}_q) \to \mathcal{F}(n, \mathbb{F}_q)\,, \quad A\,\mathrm{B}_n(\mathbb{F}_q) \mapsto A.S\,.$$

Insbesondere gilt

$$|\mathcal{F}(n, \mathbb{F}_q)| = \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathrm{B}_n(\mathbb{F}_q)|}\,.$$

Dabei gelten

$$\begin{aligned} |\mathrm{GL}_n(\mathbb{F}_q)| &= (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}) \\ &= q^{1+2+\cdots+(n-1)}(q^n - 1)(q^{n-1} - 1) \cdots (q - 1) \\ &= q^{n(n-1)/2}(q^n - 1)(q^{n-1} - 1) \cdots (q - 1) \end{aligned}$$

und

$$|\mathrm{B}_n(\mathbb{F}_q)| = (q-1)^n q^{1+2+\cdots+(n-1)} = q^{n(n-1)/2}(q-1)^n\,.$$

Also gilt

$$\begin{aligned}|\mathcal{F}(n,\mathbb{F}_q)| &= \frac{(q^n-1)(q^{n-1}-1)\cdots(q-1)}{(q-1)^n}\\ &= \prod_{k=0}^{n-1}\frac{q^k-1}{q-1} = \prod_{k=0}^{n-1}(1+q+\cdots+q^{k-1})\,.\end{aligned}$$

Lösung 34.

1. Die Aussage ist wahr: Jeder Körper ist ein Hauptidealring, und somit faktoriell (Körper sind sogar schon euklidisch). Die Aussage lässt sich auch konkret zeigen: Ist K ein Körper, so gibt es keine Primelemente in K, die leere Menge $\mathcal{P} \coloneqq \emptyset \subseteq K$ 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 Potenzreihe mit f. Sind dann $g, h \in \mathbb{Z}[\![X]\!]$ mit $g = \sum_{i=0}^\infty g_i X^i$, $h = \sum_{i=0}^\infty h_i X^i$ und $f = gh$, so gilt 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 63).

4. 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

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

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

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

6. 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 $x \in R$ ist surjektiv, induziert also einen Isomorphismus $\overline{\varphi} \colon S/\ker\varphi \to R$.

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

8. Die Aussage ist wahr: R ist noethersch, und nach iterierter Anwendung des Hilbertschen Basissatzes (siehe Übung 77) somit auch $R[X][Y] \cong R[X,Y]$.

9. Die Aussage ist falsch: Ist K ein Körper, so ist zwar $R := K[X]$ ein Hauptidealring, aber $R[Y] \cong K[X,Y]$ nicht (siehe Übung 58). Allgemeiner ist $R[X]$ genau dann ein Hauptidealring, wenn R bereits ein Körper ist (siehe Übung 61).

10. 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.

11. 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 $a_1 = a_2$.

12. Die Aussage ist falsch: Die Abbildung σ ist zwar ein Ringhomomorphismus (siehe Übung 66), aber betrachtet man etwa den Fall $R = \mathbb{F}_p[X]/(X^p)$, so gilt

$$\sigma(\overline{X}) = \overline{X}^p = \overline{X^p} = 0$$

aber $\overline{X} \neq 0$, 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.)

Lösung 35.

Wir nutzen im Folgenden wiederholt, dass ein quadratisches oder kubisches Polynom über einem Körper genau dann irreduzibel ist, wenn es eine Nullstelle hat; man siehe Übung 94.

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 ist somit irreduzibel, da es kubisch ist. 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 dem Primelement $2 \in \mathbb{Z}$.

4. Da $2 \in \mathbb{Q}$ eine Einheit ist, dürfen wir f durch 2 teilen und stattdessen das normierte Polynom $\tilde{f}(X) = X^3 - 7X + 1 \in \mathbb{Q}[X]$ betrachten. Es gibt (mindestens) zwei Möglichkeiten die Irreduziblität von $\tilde{f}$ einzusehen:
   - 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.
   - Reduzieren bezüglich des Primelements $2 \in \mathbb{Z}$ liefert $\overline{f} = X^3 + X + 1 \in \mathbb{F}_2[X]$. Da $\overline{f}(0) = \overline{f}(1) = 1$ gilt, hat $\overline{f}$ keine Nullstellen, und ist als kubisches Polynom somit irreduzibel. Also ist bereits $\tilde{f}$ irreduzibel in $\mathbb{Z}[X]$, und somit auch in $\mathbb{Q}[X]$.

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. Das Polynom ist nach Eisenstein bezüglich $3 \in \mathbb{Z}$ irreduzibel.

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

8. Die Irreduziblität ergibt sich nach Eisenstein bezüglich $3 \in \mathbb{Z}$.

9. 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 $2 \in \mathbb{Z}$ 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.

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

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

12. 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.

13. 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 des Primelements $X \in \mathbb{Q}[X]$ reduzieren, und erhalten das Polynom

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

Nach Eisenstein mit dem Primelement $p \in \mathbb{Z}$ ist $\overline{f}(Y)$ irreduzibel, also auch $\tilde{f}$, und somit auch f.

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

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

16. 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 $f(X)$.

17. Das Polynom ist nach Eisenstein bezüglich $3 \in \mathbb{Z}$ irreduzibel.

18. Reduzieren bezüglich 2 liefert das Polynom $\tilde{f}(X) \coloneqq X^3 + X + 1 \in \mathbb{F}_2[X]$. Dieses hat keine Nullstellen, und ist als kubisches Polynom somit irreduzibel. Damit ist auch f schon irreduzibel.

19. Das Polynom $f(X + 1) = X^4 + 4X^3 + 6X^2 + 4X + 2$ ist nach Eisenstein bezüglich $2 \in \mathbb{Z}$ irreduzibel, und somit ist auch f irreduzibel.

Lösung 36.

1. a) Es gilt $\mathrm{ggT}(54, 24) = 6 = 54 - 2 \cdot 24$.
   b) Es gilt $\mathrm{ggT}(270, 192) = 6 = 5 \cdot 270 - 7 \cdot 192$.
   c) Es gilt $\mathrm{ggT}(213, 168) = 3 = 15 \cdot 213 - 19 \cdot 168$.
   d) Es gilt $\mathrm{ggT}(45, 63, 105) = 3 = 36 \cdot 45 - 24 \cdot 63 - 105$.
   e) Es gilt $\mathrm{ggT}(105, 70, 42, 30) = 1 = -13 \cdot 15 + 13 \cdot 70 + 13 \cdot 42 - 3 \cdot 30$.
2. Wir wählen die größten gemeinsamer Teiler jeweils so, dass alle auftretenden Polynome ganzzahlig sind.
   a) Es gilt $\mathrm{ggT}(t^2 + t - 2, t^2 - 3t + 2) = 4t - 4 = (t^2 + t - 2) - (t^2 - 3t + 2)$.
   b) Es gilt $\mathrm{ggT}(t^2 + 3, t^2 - 3t + 2) = 28 = (-3t + 10)(t^2 + 3) + (3t - 1)(t^2 - 3t + 2)$.
   c) Es gilt $\mathrm{ggT}(t^4 - t^2 - 2t - 1, t^3 - 1) = t^2 + t + 1 = -t(t^4 - t^2 - 2t + 1) + (t^2 - 1)(t^3 - 1)$.
   d) Es gilt $\mathrm{ggT}(t^3 - t^2 + t - 1, t^3 - 3t^2 + 4t - 2) = 10t - 10$ 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 $\mathrm{ggT}(t^3 + t^2 + t + 1, t^2 - 1, t^3 - t^2 + t - 1) = 8$ mit
   $$8 = 2(t^3 + t^2 + t + 1) + (t^3 + t^2 + t + 3)(t^2 - 1) - (t^2 + 2t + 3)(t^3 - t^2 + t - 1).$$

Lösung 37.

1. Das Inverse ist 9.
2. Das Inverse ist 71.
3. Das Inverse ist 379.
4. Das Inverse ist $-\frac{1}{2}(t^4 - t^3 + t^2 - t - 1)$.
5. Das Inverse ist $\frac{1}{4}(t^2 + 2t - 1)$.
6. Das Inverse ist $-\frac{1}{3}(2t^3 - t^2 + 2t + 1)$.

Lösung 38.

1. Die Lösungsmenge ist $6 + 132\mathbb{Z}$.
2. Die Lösungsmenge ist $44 + 105\mathbb{Z}$.
3. Die Lösungsmenge ist $707 + 2310\mathbb{Z}$.
4. Die Lösungsmenge ist $\frac{5}{4}t + \frac{1}{2} + (t^2 - 4)\mathbb{Q}[t]$.

Lösung 39.
Wir bezeichnen die Ring in der gegebenen Reihenfolge mit $R_1, \dots, R_7$. Wir zeigen, dass die Isomorphieklassen der gegebenen Ringe 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_5 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 $R_1 \ncong R_4$.

Lösung 40.
1. Es gilt

$$\begin{aligned}
&\mathbb{Z}[X]/(5, 10X^4 - 3X^3 + 8X - 11) \\
\cong\, &(\mathbb{Z}[X]/(5))/((5, 10X^4 - 3X^3 + 8X - 11)/(5)) \\
=\, &(\mathbb{Z}[X]/(5))/(\overline{10X^4 - 3X^3 + 8X - 11}) \\
\cong\, &(\mathbb{Z}/(5))[X]/(10X^4 - 3X^3 + 8X - 11) = \mathbb{F}_5[X]/(10X^4 - 3X^3 + 8X - 11) \\
=\, &\mathbb{F}_5[X](2X^3 + 3X + 4) = \mathbb{F}_5[X]/(X^3 + 4X + 2).
\end{aligned}$$

Für den ersten Isomorphismus nutzen wir den dritten Isomorphiesatz. Für eine genaue Erklärung des zweiten Isomorphismus siehe man Übung 68. Für die letzte Gleichheit multiplizieren wir das Polynom mit $2^{-1} = 3$.

Durch Ausprobieren ergibt sich, dass das kubische Polynom $X^3 + 4X + 2 \in \mathbb{F}_5[X]$ keine Nullstelle hat; es ist also irreduzibel, und der Quotient $\mathbb{F}_5[X]/(X^3 + 4X + 2)$

somit ein Körper. Dabei gilt $[\mathbb{F}_5[X]/(X^3+4X+2):\mathbb{F}_5] = \deg(X^3+4X+2) = 3$, also gilt

$$\mathbb{F}_5[X]/(X^3+4X+2) \cong \mathbb{F}_{5^3} = \mathbb{F}_{125}.$$

Es gibt also 125 Elemente, von denen 124 Einheiten sind und 1 Element nilpotent ist.

2. Es gilt

$$\begin{aligned}
&\mathbb{Z}[X]/(3, 4X^3+13X^2+10X-5)\\
\cong&(\mathbb{Z}[X]/(3))/((3, 4X^3+13X^2+10X-5)/(3))\\
=&(\mathbb{Z}[X]/(3))/(\overline{4X^3+13X^2+10X-5})\\
\cong&(\mathbb{Z}/(3))[X]/(4X^3+13X^2+10X-5)\\
=&\mathbb{F}_3[X]/(4X^3+13X^2+10X-5) = \mathbb{F}_3[X]/(X^3+X^2+X+1)
\end{aligned}$$

Für den ersten Isomorphismus nutzen wir den dritten Isomorphiesatz. Für eine genaue Erklärung des zweiten Isomorphismus siehe man Übung 68.

Es ist $2 = -1$ eine Nullstelle von X^3+X^2+X+1; durch Ausmultiplizieren des entsprechenden Linearfaktors ergibt sich, dass $X^3+X^2+X+1 = (X^2+1)(X+1)$ gilt. Dabei ist das Polynom $X^2+1 \in \mathbb{F}_3[X]$ irreduzibel, da es quadratisch ist aber keine Nullstellen hat. Die obige Zerlegung ist also eine Zerlegung in irreduzible Faktoren. Nach dem chinesischen Restklassensatz ist nun

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

Der Quotient $\mathbb{F}_3[X]/(X^2+1)$ ist ein Körper, da das Polynom $X^2+1 \in \mathbb{F}_3[X]$ irreduzibel ist; dabei gilt $[\mathbb{F}_3[X](X^2+1):\mathbb{F}_3] = \deg(X^2+1) = 2$ und somit $\mathbb{F}_3 \cong \mathbb{F}_{3^2} = \mathbb{F}_9$. Ingesamt erhalten wir somit, dass

$$\mathbb{Z}[X]/(3, 4X^3+13X^2+10X-5) \cong \mathbb{F}_3 \times \mathbb{F}_9.$$

Es gibt also $3 \cdot 9 = 27$ Elemente, von denen $2 \cdot 8 = 16$ Einheiten sind und 1 Element nilpotent ist.

3. Es gilt

$$\begin{aligned}
&\mathbb{Z}[X]/(7, 3X^2+7X-14)\\
\cong&(\mathbb{Z}[X]/(7))/((7, 3X^2+7X-14)/(7))\\
=&(\mathbb{Z}[X]/(7))/(\overline{3X^2+7X-14})\\
\cong&((\mathbb{Z}/(7))[X])/(3X^2+7X-14) = \mathbb{F}_7[X]/(3X^2+7X-14)\\
=&\mathbb{F}_7[X]/(3X^2) = \mathbb{F}_7[X]/(X^2).
\end{aligned}$$

Die Familie $(1, \overline{X})$ eine $\mathbb{F}_7$-Basis von $\mathbb{F}_7[X]/(X^2)$, jedes Element $f \in \mathbb{F}_7[X]/(X^2)$ ist also von der Form $f = a + b\overline{X}$ mit eindeutigen $a, b \in \mathbb{F}_7$. Ist $a = 0$, so ist $f^2 = 0$

und f somit nilpotent. Ist $a \neq 0$, so gilt $(a+b\overline{X})(a^{-1}-ba^{-2}\overline{X}) = 1$, weshalb f eine Einheit ist. (Alternativ erkennt man, dass $a+bX$ und X^2 dann teilerfremd sind, und somit $\overline{a+bX} = a+b\overline{X}$ eine Einheit in $\mathbb{F}_7[X]/(X^2)$ ist, man siehe Übung 55.) Damit erhalten wir, dass $\mathbb{F}_7[X]/(X^2)$ aus $7^2 = 49$ Elementen besteht, von denen $6 \cdot 7 = 42$ Einheiten sind und 7 nilpotent.

Lösung 41.
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

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

Lösung 42.
Wir geben zwei mögliche Beweise an:

- 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 $\varphi = \pi_2$.
- 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 69 und Übung 70); wäre dabei $\mathfrak{p}$ maximal, so wäre dies auch $\ker\varphi$ (siehe Übung 69), also kommt jeweils 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 $\varphi = \pi_2$.

Lösung 43.
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 $y \in R$ mit $y \neq 0$ bereits $y^{n-1} = 1$, also $y \cdot y^{n-2} = 1$, weshalb y eine Einheit ist (mit $y^{-1} = y^{n-2}$). 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.

Lösung 44.

1. Die Elemente $1, \dots, n$ bilden ein Repräsentantensystem der Restklassen von $\mathbb{Z}/n$, und 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 55).

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

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

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 zu 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

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

Lösung 45.

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.

Lösung 46.

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 $R = \{\sum_i f_i T^i \in K[t] \mid f_1 = 0\}$. Also enthält 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). Folglich ist R nicht faktoriell.

Lösung 47.
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.

Lösung 48.
1. Ist $\phi\colon \mathbb{Z} \to R$ ein Ringhomomorphismus, so gilt $\phi(1_\mathbb{Z}) = 1_R$. Für alle $n \in \mathbb{Z}$ gilt deshalb

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

   Also ist ϕ eindeutig. Durch direktes Nachrechnen ergibt sich auch, dass $\psi\colon \mathbb{Z} \to R$ mit

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

   ein Ringhomomorphismus ist.

2. Es gibt einen eindeutigen Ringhomomorphismus $\phi\colon \mathbb{Z} \to Z$ sowie einen eindeutigen Ringhomomorphismus $\psi\colon Z \to \mathbb{Z}$. Es ist auch $\psi \circ \phi\colon \mathbb{Z} \to \mathbb{Z}$ ein Ringhomomorphismus. Die Identität $\mathrm{id}_\mathbb{Z}\colon \mathbb{Z} \to \mathbb{Z}$ ist ebenfalls ein Ringhomomorphismus. Da es genau einen Ringhomomorphismus $\mathbb{Z} \to \mathbb{Z}$ gibt, müssen 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 auch, dass $\phi \circ \psi = \mathrm{id}_Z$ gilt.

Lösung 49.
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, deshalb bereits $\varepsilon_1\varepsilon_2 = 1$. Also ist ε_1 eine Einheit mit $\varepsilon_1^{-1} = \varepsilon_2$. Da $y = \varepsilon_1 x$ gilt, ist somit $x \sim y$.

Lösung 50.

1. Für je zwei Einheiten $x, y \in R^\times$ ist auch xy eine Einheit, also $xy \in R^\times$, da

$$(xy)(y^{-1}x^{-1}) = xyy^{-1}x^{-1} = xx^{-1} = 1$$

gilt. 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 $x \in R^\times$ 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.

Lösung 51.

1. Es genügt den Fall zu betrachten, dass $\mathfrak{p}$ ein echtes Ideal ist, denn dies ist äquivalent dazu, dass $R/\mathfrak{p} \neq 0$ gilt.

Für alle $x \in R$ sei $\overline{x} \in R/\mathfrak{p}$ die entsprechende Äquivalenzklasse. Der Ring $R/\mathfrak{p}$ ist genau dann ein Integritätsbereich, 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 zu der Aussage

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

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

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

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 53). Der Ring $R/\mathfrak{m}$ ist genau dann ein Körper, wenn $R/\mathfrak{m}$ genau zwei Ideale enthält (siehe Übung 92); 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.

Lösung 52.
Es sei $\pi\colon S \to S/\mathfrak{a}$, $s \mapsto \overline{s}$ die kanonische Projektion.

1. Dann ist $\pi \circ \phi$ ein Ringhomomorphismus und somit

$$\ker(\pi \circ \phi) = (\pi \circ \phi)^{-1}(0) = \phi^{-1}(\pi^{-1}(0)) = \phi^{-1}(\ker \pi) = \phi^{-1}(\mathfrak{a})$$

ein Ideal in R.

2. Die Aussage gilt: Es sei $\mathfrak{q} \coloneqq \phi^{-1}(\mathfrak{p})$. Der Quotient $S/\mathfrak{p}$ ist ein Integritätsbereich, da $\mathfrak{p}$ ein Primideal ist. Nach dem vorherigen Aufgabenteil ist $\mathfrak{q}$ ein Ideal in R, und da

$$\ker(\pi \circ \phi) = \phi^{-1}(\ker \pi) = \phi^{-1}(\mathfrak{p}) = \mathfrak{q}$$

gilt, induziert $\pi \circ \phi$ einen injektiven Ringhomomorphismus

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

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

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

Lösung 53.

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 52). 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 $\overline{r} \cdot \overline{x} = \overline{rx} \in \pi(J)$.

   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 in R/I.

   Für jedes Ideal $J \subseteq R$ gilt $\pi^{-1}(\pi(J)) = J + I$: Es gilt $J \subseteq \pi^{-1}(\pi(J))$ 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 $y \in J$ 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 nun 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 $J \supseteq I$. Insbesondere 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.

Lösung 54.

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 53). Das Ideal J' ist endlich erzeugt, also $J' = (a_1, \ldots, a_n)$, da R noethersch ist. Damit gilt $J = J'/I = (\overline{a_1}, \ldots, \overline{a_n})$, 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 dem Ring $K[X]/(X^2)$ 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.

Lösung 55.

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

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

(siehe Übung 53). 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 $(x) + I = R$.

Lösung 56.

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

   Es gilt $0 \in I$, da $0/1 \in J$. Für $x_1, x_2 \in I$ gelten $x_1/1, x_2/1 \in J$ und somit auch $(x_1 + x_2)/1 = x_1/1 + x_2/1 \in J$, also $x_1 + x_2 \in I$. Für $x \in I$ und jedes $r \in R$ gilt $x/1 \in J$ und somit auch $(rx)/1 = (r/1)(x/1) \in J$, also $rx \in I$. 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 in R (siehe Übung 52).

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

2. Für alle $i \in I$ gilt wegen $a_i \in I$ auch $a_i/1 \in I_S$. Deshalb gilt $(a_i/1 \mid i \in I) \subseteq I_S$. Ist andererseits $x/s \in I_S$ mit $x \in I$, so gibt es eine Linearkombination $x = \sum_{i \in I} r_i a_i$ mit $r_i = 0$ für fast alle $i \in I$. Deshalb gilt $x/s = \sum_{i \in I}(r_i/s)(a_i/1) \in (a_i \mid i \in I)$. 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 $I \subseteq R$. Das Ideal I ist endlich erzeugt, also $I = (a_1, \ldots, a_n)$, da R noethersch ist. Nach dem zweiten Aussagenteil gilt deshalb $J = I_S = (a_1/1, \ldots, a_n/1)$, weshalb J endlich erzeugt. Es ist also jedes Ideal in R_S endlich erzeugt, und R_S somit 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.

Lösung 57.

1. Das Radikal $\sqrt{I}$ ist als $\sqrt{I} = \{x \in R \mid \text{es gibt } n \in \mathbb{N} \text{ mit } x^n \in I\}$ definiert.

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

   Insbesondere ist somit $0 \in \sqrt{I}$, da $0 \in I$ gilt. Für $x, y \in \sqrt{I}$ gibt es $n, m \in \mathbb{N}$ mit $x^n, y^m \in I$. Für alle $k = 0, \ldots, n+m$ gilt deshalb $x^k \in I$ oder $y^{n+m-k} \in I$, und somit auch
   $$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k} \in I.$$
   Deshalb ist auch $x + y \in \sqrt{I}$. Für $r \in R$ und $x \in \sqrt{I}$ gibt es $n \in \mathbb{N}$ mit $x^n \in I$, womit auch $(rx)^n = r^n x^n \in I$ gilt. Somit ist auch $rx \in \sqrt{I}$.

3. 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 $(x^n)^m \in I$. Somit gilt $x^{nm} \in I$, also $x \in \sqrt{I}$, weshalb auch $\sqrt{\sqrt{I}} \subseteq \sqrt{I}$ gilt.

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

5. Aus den Inklusionen $I \cap J \subseteq I, J$ folgen die Inklusionen $\sqrt{I \cap J} \subseteq \sqrt{I}, \sqrt{J}$ und hieraus 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 $x^m \in J$. Deshalb gilt $x^{n+m} = x^n x^m \in I \cap J$ (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 somit $x \in \sqrt{I \cap J}$.

6. Gilt $I = \sqrt{I}$ so erfüllt I die definierende Eigenschaft eines Radikalideals (mit $J = I$). Ist andererseits $I = \sqrt{J}$ für ein beliebiges Ideal $J \subseteq R$, so gilt $\sqrt{I} = \sqrt{\sqrt{J}} = \sqrt{J} = I$.

7. Der Quotient R/I ist genau reduziert, wenn die Implikation
   $$\text{es gibt } n \in \mathbb{N} \text{ mit } \overline{x}^n = 0 \implies \overline{x} = 0 \qquad \text{für alle } x \in R \tag{4}$$
   gilt. 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 die Implikation (4) äquivalent zu der Implikation
   $$\text{es gibt } n \in \mathbb{N} \text{ mit } x^n \in I \implies x \in I \qquad \text{für alle } x \in R. \tag{5}$$
   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 stets $I \subseteq \sqrt{I}$ gilt, ist dies äquivalent dazu, dass $I = \sqrt{I}$, dass also I ein Radikalideal ist.

8. Wir geben zwei mögliche (äquivalente) Argumentation an:

- Für $x \in \sqrt{\mathfrak{p}}$ gibt es ein $n \geq 1$ mit $x^n \in \mathfrak{p}$. Da $\mathfrak{p}$ ein Primideal ist, folgt aus $x^n \in \mathfrak{p}$, dass bereits $x \in \mathfrak{p}$ gilt. Also gilt $\sqrt{\mathfrak{p}} \subseteq \mathfrak{p}$ und somit $\mathfrak{p} = \sqrt{\mathfrak{p}}$.
- Der Quotient $R/\mathfrak{p}$ ist ein Integritätsbereich, da $\mathfrak{p}$ ein Primideal ist. Für jedes $x \in R/\mathfrak{p}$ mit $x^n = 0$ folgt aus der Nullteilerfreiheit von $R/\mathfrak{p}$, dass bereits $x = 0$ gilt. Somit ist der Ring $R/\mathfrak{p}$ reduziert, und deshalb $\mathfrak{p}$ ein Radikalideal in R.

Lösung 58.

1. Wäre $(X, Y) = (f)$ für ein $f \in K[X, Y]$, so würde $f \mid X$ und $f \mid Y$ gelten, also f ein gemeinsamer Teiler von X und Y sein (sogar schon ein größter gemeinsamer Teiler, siehe Übung 74). Da X und Y teilerfremd sind, müsste f bereits eine Einheit in $K[X, Y]$ sein; dann würde aber $(X, Y) = (f) = (1) = K[X, Y]$ gelten, was nicht der Fall ist (denn $K[X, Y]/(X, Y) \cong K \neq 0$).

2. Es sei $R \coloneqq K[X_i \mid i = 1, 2, 3, \dots]$. Wir nehmen an, dass $I \coloneqq (X_i \mid i \in \mathbb{N})$ von $f_1, \dots, f_t \in I$ erzeugt wird. Es gilt $I = \bigcup_{n \geq 1}(X_1, X_2, \dots, X_n)$, weshalb es ein $N \geq 1$ mit $f_1, \dots, f_t \in (X_1, \dots, X_N)$ gibt. Es gilt also

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

und somit $I = (X_1, \dots, X_N)$. Deshalb würde

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

gelten, aber R ist kein Körper.

Lösung 59.

Als euklidischer Ring ist R insbesondere ein Integritätsbereich.

Es sei $g \setminus \{0\} \colon R \to \mathbb{N}$ die Gradabbildung und $I \subseteq R$ ein Ideal. Im Fall $I = 0$ gilt $I = (0)$, wir betrachten daher im Folgenden nur 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 $x \neq 0$. Zum einen gilt $(a) \subseteq I$. Für $x \in I$ gibt es andererseits $q, r \in R$ mit $x = qa + r$, so dass entweder $r = 0$ oder $g(r) < g(a)$ gilt. Da $r = x - qa \in I$ gilt, kann der Fall $g(r) < g(a)$ wegen der Minimalität von a nicht eintreten. Also ist $r = 0$ und somit $x = qa \in (a)$. Das zeigt, dass auch $I \subseteq (a)$ gilt, und somit insgesamt $I = (a)$.

Lösung 60.

Es sei $p \in R$ mit $\mathfrak{m} = (p)$. Wegen $\mathfrak{m} \neq 0$ gilt dabei $p \neq 0$, weshalb p prim ist. 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 dabei bereits $p \mid a$ oder $p \mid b$.

Gilt $p \mid b$, so gibt es $c \in R$ mit $b = cp$. Dann gilt $p = ab = acp$ und somit $1 = ac$, 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 gilt $\mathfrak{a} = (a) \subseteq (p) = \mathfrak{m}$, und somit bereits $\mathfrak{m} = \mathfrak{a}$.

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

Lösung 61.
Wir bemerken zunächst, dass $K \neq 0$ gilt, da $0[X] = 0$ kein Hauptidealring ist. Wir bemerken außerdem das Folgende:

Behauptung. Die übliche Gradabbildung $\deg\colon K[X] \to \{-\infty\} \cup \mathbb{N}$ 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. □

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 $(a, X) = (f)$.

Insbesondere gilt $f \mid a$. Aus $\deg a = 0$ ergibt sich mit der Additivität des Grades, dass auch $\deg f = 0$ gilt, also $f \in K$ mit $f \neq 0$.

Außerdem gilt $f \mid X$. Wegen $f \in K$ erhalten wir aus der Additivität des Grades, dass es $bX + c \in K[X]$ mit $b \neq 0$ gibt, so dass $X = f \cdot (bX + c)$ gilt. Dann gilt $1 = fb$, weshalb f eine Einheit ist.

Somit gilt $(a, X) = (f) = (1) = K[X]$. Inbesondere gibt es $g, h \in K[X]$ mit $1 = ag + Xh$. Somit gilt $1 = ag_0$, weshalb a eine Einheit in K ist.

Das zeigt, dass jedes $a \in K$ mit $a \neq 0$ eine Einheit in K ist; also ist K ein Körper.

Bemerkung. Die obige Argumentation zeigt für einen beliebigen kommutativen Ring R, dass (a, X) für $a \in R$ genau dann ein Hauptideal ist, wenn $a \in R^\times$ gilt. Somit ist beispielsweise $(2, X) \subseteq \mathbb{Z}[X]$ kein Hauptideal.

Lösung 62.

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

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

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

$$(e+n)^{-1} = e^{-1}(1+e^{-1}n)^{-1} = e^{-1}\sum_{p=0}^{\infty}(-1)^p(e^{-1}n)^p = \sum_{p=0}^{\infty}(-1)^p e^{-1-p}n^p.$$

Lösung 63.
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 insgesamt $fg = 1$.

Lösung 64.
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 gilt

$$1 = |1|^2 = |zz^{-1}|^2 = |z|^2 |z^{-1}|^2. \tag{6}$$

Für alle $w \in \mathbb{Z}[i]$ gilt $w = a + ib$ mit $a, b \in \mathbb{Z}$, und deshalb $|w|^2 = a^2 + b^2 \in \mathbb{Z}$. In (6) 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 $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

Lösung 65.
Wir nehmen an, dass fg nicht primitiv ist. Da R faktoriell ist, gibt es dann 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. Deshalb ist auch $(R/(p))[T]$ ein Integritätsbereich. Aus $0 = \varphi(f)\varphi(g)$ folgt deshalb, dass $\varphi(f) = 0$ oder $\varphi(g) = 0$ gilt. 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.

Lösung 66.
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

$$\sigma(x + y) = (x + y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} \tag{7}$$

Für alle $k = 1, \ldots, p-1$ gilt dabei $p \mid \binom{p}{k}$, denn der Zähler von $\binom{p}{k} = p!/(k!(p-k)!)$ enthält dann den Primfaktor p, der Nenner aber nicht. Folglich vereinfacht sich (7) 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 $x = 0$ gilt. Also ist σ injektiv, und wegen der Endlichkeit von R damit auch schon bijektiv.

Lösung 67.
Es sei $R = \mathbb{Z} \times \mathbb{Z}$ und $S = \mathbb{Z} \times 0 = \{(n, 0) \mid n \in \mathbb{Z}\}$. Die Teilmenge $S \subseteq R$ ist abgeschlossen unter Addition und Multiplikation und bildet mit den Einschränkungen dieser Operationen einen kommutativen Ring, für den $S \cong \mathbb{Z}$ gilt. Da $1_R = (1, 1) \notin S$ gilt, ist S allerdings kein Unterring von R.

Lösung 68.
1. Die kanonische Projektion $\pi\colon R \to R/\mathfrak{a}$, $x \mapsto \overline{x}$ induziert einen Ringhomomorphismus $\varphi\colon R[X] \to (R/\mathfrak{a})[X]$ mit

$$\varphi\left(\sum_i f_i X^i\right) = \sum_i \pi(f_i) X^i = \sum_i \overline{f_i} X^i \qquad \text{für alle } \sum_i f_i X^i \in R[X].$$

   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 $\ker \varphi = \mathfrak{a}[X]$, 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 $\mathfrak{p}[X]$ ein Primideal.

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 $\mathfrak{m}[X]$ nie 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 45).

5. Es gilt $\mathfrak{a} \subseteq \mathfrak{a}[X]$ und somit $(\mathfrak{a})_{R[X]} \subseteq \mathfrak{a}[X]$. Andererseits gilt $aX^i \in (\mathfrak{a})_{R[X]}$ für jedes $a \in \mathfrak{a}$ und $i \geq 0$ und somit $\sum_i a_i X^i \in (\mathfrak{a})_{R[X]}$ 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, weshalb $\mathbb{F}_3[X]/(X^2+1) \cong \mathbb{F}_9$ gilt. 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.

Lösung 69.

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

2. Da die π_i surjektiv sind, ist es auch π. Da $\ker \pi = \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n$ gilt, induziert π also einen Isomorphismus
$$\begin{aligned}\overline{\pi} \colon (R_1 \times \cdots \times R_n)/(\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n) &\to (R_1/\mathfrak{a}_1) \times \cdots \times (R_n/\mathfrak{a}_n),\\ \overline{(x_1, \dots, x_n)} &\mapsto (\overline{x_1}, \dots, \overline{x_n}).\end{aligned}$$

3. Gilt $\mathfrak{a}_i \neq R_i$ 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, weshalb der Ring nicht nullteilerfrei ist. Es genügt daher, sich auf den Fall einzuschränken, dass $\mathfrak{a}_i = R_i$ für alle $i = 1, \dots, n$ bis auf ein $1 \leq j \leq n$ gilt. 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.

Lösung 70.
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 $\mathfrak{a}_i \coloneqq \pi_i(\mathfrak{a})$.

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

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

Lösung 71.

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

   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 $\varphi \circ j = i \times i'$ gilt, 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 $0 = \varphi((r, r')/(s, s')) = (r/s, r'/s')$. Da $r/s = 0/1$ gilt, gibt es $t \in S$ mit $tr = 0$. Analog gibt es auch $t' \in S'$ mit $t'r' = 0$.

   Für $(t, t') \in S \times S'$ ist dann $(t, t')(r, r') = (tr, t'r') = 0$, weshalb $(r, r')/(s, s') = 0$ gilt. Also ist $\ker \varphi = 0$ und φ somit auch injektiv.

Lösung 72.

1. Da $1 \in S$ gilt, ist auch $1 = f(1) \in f(S) = S'$. Für $s_1', s_2' \in S'$ gibt es $s_1, s_2 \in S$ mit $s_1' = f(s_1)$ und $s_2' = f(s_2)$. Dann gilt auch $s_1 s_2 \in S$ und somit

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

2. 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:

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

Lösung 73.

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

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

gilt. Nach der universellen Eigenschaft der Lokalisierung R_f induziert der Ringhomomorphismus $R \to R[X] \to R[X]/(fX-1)$, $r \mapsto \overline{r}$ einen Ringhomomorphismus

$$\varphi \colon R_f \to R[X]/(fX-1) \quad \text{mit} \quad \varphi\left(\frac{r}{f^k}\right) = \frac{\overline{r}}{\overline{f}^k} = \overline{r}\overline{X}^k = \overline{rX^k}.$$

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 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 gilt

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

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 $\varphi^{-1} = \psi$.

Lösung 74.

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, gibt es eine Linearkombination $a = \sum_{i \in I} r_i a_i$ 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 $(X, Y) \subsetneq (1)$.

Lösung 75.

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

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

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

Lösung 76.

Es sei

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

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 $\mathcal{I}$ 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 $\mathfrak{m} \subsetneq \mathfrak{m}'$ gilt, stünde dies im Widerspruch zur Maximalität von $\mathfrak{m}$ in $\mathcal{I}$. Also muss $\mathfrak{m}$ bereits ein maximales Ideal in R sein.

Lösung 77.
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

$$I_d \coloneqq \left\{ a \in R \,\middle|\, \text{es gibt ein Polynom } \sum_{i=0}^{d} a_i X^i \in I \text{ mit } a_d = a \right\}.$$

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

Für $a \in I_d$ gibt es $f = \sum_{i=0}^{d} a_i X^i \in I$ mit $a = a_d$. Dann ist $Xf = \sum_{i=1}^{d+1} a_{i+1} X^i \in I$, und somit $a \in I_{d+1}$. 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 $I_D = I_{D+k}$ für alle $k \geq 0$.

Die Ideale $I_0, \ldots, I_D$ sind endlich erzeugt, da R noethersch sind. Für jedes $d = 0, \ldots, D$ sei $I_d = (a_1^{(d)}, \ldots, a_{s_d}^{(d)})$. Für jedes $d = 0, \ldots, D$ und $i = 1, \ldots, s_d$ gibt es dann ein Polynom $f_i^{(d)} = \sum_{j=0}^{d} a_i X^j \in I$ mit $a_d = a$. Man merke für $d = 0$, dass $f_i^{(0)} = a_i^{(0)}$ für alle $i = 0, \ldots, d$ gilt, da ein konstantes Polynom mit seiem Leitkoeffizienten übereinstimmt. Es sei $J \coloneqq (f_i^{(d)} \mid d = 0, \ldots, D, i = 1, \ldots, s_d) \subseteq I$.

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

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

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 $\deg g < d$. Es sei $a \in I_d$ der Leitkoeffizient von f. Wir unterscheiden zwischen zwei Fällen:

- Gilt $d \leq D$, so gilt $a \in I_d = (a_1^{(d)}, \ldots, a_{s_d}^{(d)})$, 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 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 $f - X^{d-D} g \in I$ 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 $f \in J$ gilt.

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

Lösung 78.
Wir geben zwei mögliche Beweise an:

1. Der Ring $K[\![X]\!]$ ist euklidisch mit der üblichen Gradabbildung $\operatorname{Deg}\colon K[\![X]\!] \to \mathbb{N} \cup \{\infty\}$ 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 $f = \sum_{i=n}^{\infty} f_i X^i$ für ein $n \geq 0$ mit $f_n \neq 0$. Dann ist

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

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

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

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

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

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

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

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

   Gebe es ein maximales Ideal $\mathfrak{m}' \subseteq K[\![X]\!]$ mit $\mathfrak{m}' \neq \mathfrak{m}$, so würde wegen der Maximalität von $\mathfrak{m}'$ inbesondere $\mathfrak{m}' \nsubseteq \mathfrak{m}$ gelten. Dann gebe es $f \in \mathfrak{m}'$ mit $f \notin \mathfrak{m}$, also $f_0 \neq 0$ und somit $f_0 \in K^\times$. 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.

Lösung 79.

1. Die Aussage ist falsch: Man betrachte $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt[3]{2})$. Jeder Automorphismus $\sigma \in \operatorname{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ muss die Nullstellen des Polynoms $f(X) \coloneqq X^3 - 2 \in \mathbb{Q}[X]$ 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 $\zeta = e^{2\pi i/3}$). Dabei gilt $\zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2} \notin \mathbb{R}$. 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 $\sigma \in \operatorname{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ 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 103.

4. Die Aussage ist falsch: Siehe Übung 103.

5. Die Aussage ist falsch, denn sonst wäre

$$3 = [\mathbb{F}_{2^3} : \mathbb{F}_2] = [\mathbb{F}_8 : \mathbb{F}_2] \mid [\mathbb{F}_{32} : \mathbb{F}_2] = [\mathbb{F}_{2^5} : \mathbb{F}_2] = 5.$$

6. Die Aussage ist falsch: Sie gilt genau dann, wenn die Erweiterung L/K algebraisch ist, siehe Übung 96. Als Gegenbeispiel betrachte man somit beispielsweise $L = K(t)$.

7. Die Aussage ist wahr: Sie wurde auf einem der Übungszettel gezeigt, wir geben hier der Vollständigkeit halber dennoch einen Beweis an:

   Wir zeigen die Aussage per Induktion über n. Für $n = 1$ gilt $L = K$ und die Aussage gilt. Es sei nun $n \geq 2$, und die Aussage gelte für alle Polynome vom Grad $< n$.

   Wir betrachten zunächst den Fall, dass $f(t)$ irreduzibel ist. Dann sei $a \in L$ eine Nullstelle von $f(t)$. Dann ist $f(t)$ das Minimalpolynom von a über K und deshalb $[K(a) : K] = n$. Über $K(a)$ lässt sich von $f(t)$ der Linearfaktor $(t-a)$ abspalten, d.h. es gibt ein Polynom $g(t) \in K(a)[t]$ mit $f(t) = g(t)(t - a)$. Dabei gilt insbesondere $\deg g(t) = \deg f(t) - 1 = n - 1$. Dann ist L auch von $g(t)$ ein Zerfällungskörper, und nach Induktionsvoraussetzung gilt deshalb $[L : K(a)] \mid (n-1)!$. Zusammen mit $[K(a) : K] = n$ erhalten wir, dass

$$[L : K] = [L : K(a)][K(a) : K] \mid (n-1)!\, n = n!\,.$$

   Allgemeiner sei $g(t)$ ein irreduzibler Faktor von $f(t)$, und es sei $h(t) \in K[t]$ mit $f(t) = g(t)h(t)$. Sind dabei $d_1 := \deg g(t)$ und $d_2 := \deg h(t)$, so gilt $n = d_1 + d_2$. Es enthält L einen Zerfällungskörper L' von $g(t)$. Fassen wir $h(t)$ als ein Polynom über L' auf, also als $h(t) \in L'[t]$, so ist L ein Zerfällungskörper von $h(t)$ über L'. Nach Induktionsvoraussetzung gelten nun

$$[L' : K] \mid d_1! \quad \text{and} \quad [L : L'] \mid d_2!\,,$$

   und somit

$$[L : K] = [L : L'][L' : K] \mid d_1!\, d_2! \mid (d_1 + d_2)! = n!\,.$$

   (Es ist $d_1!\, d_2!$ ein Teiler von $(d_1 + d_2)!$, da $(d_1 + d_2)!/(d_1!d_2!) = \binom{d_1+d_2}{d_1}$ ganzzahlig ist.)

8. Die Aussage ist wahr: Sind $\alpha_1, \dots, \alpha_d \in L$ mit $d \leq n$ die paarweise verschiedenen Nullstellen von f, so muss jedes $\sigma \in \mathrm{Gal}(L/K)$ die Nullstellen von f permutieren. Also gibt es eine Einbettung $\varphi\colon \mathrm{Gal}(L/K) \to S_d$, $\sigma \mapsto \pi_\sigma$ wobei $\pi_\sigma \in S_d$ die eindeutige Permutation ist, so dass $\sigma(\alpha_i) = \alpha_{\pi_\sigma(i)}$ für alle $i = 1, \dots, d$ gilt. Da $\operatorname{im}\varphi \subseteq S_d$ eine Untergruppe ist, erhalten wir, dass

$$|\mathrm{Gal}(L/K)| = |\operatorname{im}\varphi| \mid |S_d| = d! \mid n!.$$

9. Die Aussage ist wahr: Da L_1/K und L_2/K algebraisch sind, werden beide Erweiterungen von algebraischen ELementen erzeugt. Es gilt also

$$L_1 = K(\alpha_i \mid i \in I) \quad \text{und} \quad L_2 = K(\beta_j \mid j \in J)$$

für Elemente $\alpha_i \in L_1$ und $\beta_j \in L_2$, die jeweils algebraisch über K sind. Dann gilt $L_1L_2 = K(\alpha_i, \beta_j \mid i \in I, j \in J)$, weshalb auch L_1L_2/K von algebraischen Elementen erzeugt wird, also algebraisch ist.

Lösung 80.

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 $p = q$.

Lösung 81.

1. Das Polynom $f(X) \coloneqq X^3 - 6X^2 + 9X + 3 \in \mathbb{Q}[X]$ 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 gelten auch die Gleichungen $\alpha^5 = 6\alpha^4 - 9\alpha^3 - 3\alpha^2$ und $\alpha^4 = 6\alpha^3 - 9\alpha^2 - 3\alpha$. Durch sukzessives Einsetzen ergibt sich damit, 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

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

Lösung 82.
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 zyklischen Erzeuger sind genau die $\alpha \in L$, für die $\alpha \notin K$.

Lösung 83.
1. Da $K(\alpha^2) \subseteq K(\alpha)$ gilt, genügt es zu zeigen, dass $\alpha^2 \in K(\alpha)$ gilt. Wir nehmen an, dass $\alpha^2 \notin K(\alpha)$ gelten würde. 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.

2. 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

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

   was nicht seien kann.

Lösung 84.
Sind α und β algebraisch über K, so ist $K(\alpha,\beta)/K$ eine algebraische Körpererweiterung. Da $\alpha+\beta, \alpha\beta \in K(\alpha,\beta)$ gilt, sind dann auch $\alpha+\beta$ und $\alpha\beta$ 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.

Lösung 85.
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 $L \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$ gilt 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 $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$ gilt). 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 $\sqrt{3} = (3-a^2-2b^2)/(ab) \in \mathbb{Q}$, 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 $f \in \mathbb{Q}[X]$ bereits galoisch über $\mathbb{Q}$.

4. Da $L/\mathbb{Q}$ galoisch ist, wissen wir, dass $|\mathrm{Gal}(L/\mathbb{Q})| = [L:\mathbb{Q}] = 4$ gilt. 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 $\sigma(\sqrt{3}) = \pm\sqrt{3}$ gelten. 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

$$\sigma_1 \colon \begin{cases} \sqrt{2} \mapsto \sqrt{2}, \\ \sqrt{3} \mapsto \sqrt{3}, \end{cases} \quad \sigma_2 \colon \begin{cases} \sqrt{2} \mapsto -\sqrt{2}, \\ \sqrt{3} \mapsto \sqrt{3}, \end{cases}$$
$$\sigma_3 \colon \begin{cases} \sqrt{2} \mapsto \sqrt{2}, \\ \sqrt{3} \mapsto -\sqrt{3}, \end{cases} \quad \sigma_4 \colon \begin{cases} \sqrt{2} \mapsto -\sqrt{2}, \\ \sqrt{3} \mapsto -\sqrt{3}, \end{cases}$$

   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.

Lösung 86.

1. Es gilt $L = \mathbb{Q}(\sqrt[3]{3}, \zeta\sqrt[3]{3}, \zeta^2\sqrt[3]{3})$ da $\zeta = (\zeta\sqrt[3]{3})/\sqrt[3]{3}$ gilt. Also wird L über $\mathbb{Q}$ von den Nullstellen des Polynoms $f(X) \coloneqq X^3 - 3 \in \mathbb{Q}[X]$ erzeugt, ist also ein Zerfällungskörper von f. Die Nullstellen von f sind paarweise verschieden, also ist f separabel. Als Zerfällungskörper eines separablen Polynoms ist $L/\mathbb{Q}$ galoisch.

2. Wir betrachten den Zwischenkörper $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{3}) \subseteq L$. Nach Eisenstein bezüglich $3 \in \mathbb{Z}$ ist f irreduzibel. Also ist f das Minimalpolynom von $\sqrt[3]{3}$, und somit $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = \deg f = 3$. Außerdem gilt $\zeta \notin \mathbb{R} \supseteq L$. Es gilt nun (mindestens) zwei Argumentationen:

   - Aus $\zeta \notin \mathbb{Q}(\sqrt[3]{3})$ ergibt sich, dass $[L : \mathbb{Q}(\sqrt[3]{3})] \geq 2$. Zusammen mit $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$ erhalten wir, dass $[L:\mathbb{Q}] \geq 6$ gilt. Andererseits ist L ein Zerfällungskörper eines kubischen Polynoms, weshalb $[L:\mathbb{Q}] \mid 3! = 6$ gilt. Zusammen erhalten wir, dass $[L:\mathbb{Q}] = 2$.
   - Es gilt $L = \mathbb{Q}(\sqrt[3]{3}, \zeta) = \mathbb{Q}(\sqrt[3]{3}, \zeta\sqrt[3]{3}) = \mathbb{Q}(\sqrt[3]{3})(\zeta\sqrt[3]{3})$. Das Polynom

$$g(X) \coloneqq (X - \zeta\sqrt[3]{3})(X - \zeta^2\sqrt[3]{3}) = f(X)/(X - \sqrt[3]{3}) \in \mathbb{Q}(\sqrt[3]{3})[X]$$

     ist irreduzibel, da wegen $\zeta \notin \mathbb{Q}(\sqrt[3]{3})$ auch $\zeta\sqrt[3]{3}, \zeta\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{3})$ gilt. Somit ist g das Minimalpolynom von $\zeta\sqrt[3]{3}$ über $\mathbb{Q}(\sqrt[3]{3})$ und deshalb $[L : \mathbb{Q}(\sqrt[3]{3})] = 2$. Zusammen mit $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$ erhalten wir, dass $[L:\mathbb{Q}] = 6$ gilt.

3. Es ist L der Zerfällungskörper von f und $[L:\mathbb{Q}] = 6 = 3! = (\deg f)!$. Aus der Vorlesung ist bekannt, dass deshalb bereits $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$ gilt. Aus $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$ erhalten wir inbesondere, dass $\mathrm{Gal}(L/\mathbb{Q})$ nicht abelsch ist.

   Von Hand lässt sich die Aussage wie folgt nachrechnen: Jedes $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ muss die Nullstellen von f, also $z_1 = \sqrt[3]{3}$, $z_2 = \zeta\sqrt[3]{3}$ und $z_3 = \zeta^2\sqrt[3]{3}$, permutieren. Da L bereits von diesen Nullstellen erzeugt wird, ergibt sich eine Einbettung

$\varphi\colon \mathrm{Gal}(L/\mathbb{Q}) \to S_3$, wobei $\pi = \varphi(\sigma)$ die eindeutige Permutation mit $\sigma(z_i) = z_{\pi(i)}$ für alle $i = 1, 2, 3$ ist. Da $L/\mathbb{Q}$ galoisch ist, gilt dabei

$$|\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 6 = 3! = |S_3|$$

weshalb φ bereits bijektiv, und somit ein Isomorphismus ist.

Lösung 87.

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

   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 ein Zerfällungskörper des separablen Polynoms $f \in \mathbb{Q}[X]$, und $L/\mathbb{Q}$ somit galoisch.

3. Da $L/\mathbb{Q}$ Galoisch ist gilt $|\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 8$. Da $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ 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 $|\mathrm{Gal}(L/\mathbb{Q})| = 8$ erhalten wir somit, dass die Automorphismen $\sigma_{r,s} \in \mathrm{Gal}(L/\mathbb{Q})$ 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, d.h. zur Symmetriegruppe des Quadrates. Die Gruppe $\mathrm{Gal}(L/\mathbb{Q}$ selbst lässt sich hier als Symmetriegruppe des Quadrates mit Eckpunkten $\sqrt[2]{4}, i\sqrt[2]{4}, -\sqrt[2]{4}, -i\sqrt[2]{4}$ verstehen.)

Lösung 88.

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 $\tilde{f}(0) = \tilde{f}(1) = 1$ gilt 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 $f(\alpha(\alpha-2)) = \cdots = 0$. Alternativ ergibt sich mithilfe von Polynomdivision, dass

$$\alpha^6 t - 6\alpha^5 + 10\alpha^4 - 9\alpha^2 + 2\alpha + 1 = (\alpha^3 - 4\alpha^2 + 3\alpha + 1)\underbrace{(\alpha^3 - 2\alpha^2 - \alpha + 1)}_{=0} = 0.$$

3. Da $\mathrm{char}\,\mathbb{Q} = 0$ 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 $\operatorname{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong \mathbb{Z}/3$.

Lösung 89.
Es sei $G \coloneqq \operatorname{Gal}(L/K)$. Jedes $\sigma \in G$ induziert einen Automorphismus $\varphi_\sigma \colon L[X] \to L[X]$, $\sum_i a_i X^i \mapsto \sum_i \sigma(a_i) X^i$. Jedes $\sigma \in G$ muss die Nullstellen von f permutieren; es gibt also eine Permutation $\pi_\sigma \in S_n$ mit $\sigma(\alpha_i) = \alpha_{\pi_\sigma(i)}$ für alle $i = 1, \dots, n$. Für jedes $\sigma \in G$ gilt deshalb

$$\begin{aligned}\varphi_\sigma(g(X)) &= \varphi_\sigma\left(\prod_{i=1}^{n} X - \alpha_i\right) = \prod_{i=1}^{n}(X - \sigma(\alpha_i)) \\ &= \prod_{i=1}^{n}(X - \alpha_{\pi_\sigma(i)}) = \prod_{j=1}^{n}(X - \alpha_j) = g(X).\end{aligned}$$

Also ist g invariant unter allen φ_σ mit $\sigma \in G$. Da die φ_σ koeffizientenweise agieren, erhalten wir, dass alle Koeffizienten von g invariant unter allen $\sigma \in G$ sind. Die Koeffizienten von G liegen also im Fixkörper L^G, und g somit in $L^G[X]$. Da L/K galoisch ist, gilt dabei bereits $L^G = K$.

Lösung 90.
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 $x < z < y$ gilt, wenn $\sigma(x) < \sigma(z) < \sigma(y)$ gilt; also bildet σ offene Intervalle auf offene Intervalle ab. Da eine jede offene Menge $U \subseteq \mathbb{R}$ eine Vereinigung offener Intervalle ist, folgt daraus, dass auch $\sigma(U) \subseteq \mathbb{R}$ offen ist. Wendet man dieses Resultat auf $\sigma^{-1} \in \operatorname{Gal}(\mathbb{R}/\mathbb{Q})$ 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.

Lösung 91.
1. Über $\mathbb{C}$ zerfällt f in Linearfaktoren, und die Nullstellen sind $\sqrt[6]{2}, \zeta\sqrt[6]{2}, \dots, \zeta^{p-1}\sqrt[6]{2}$. Es gilt $L = \mathbb{Q}(\sqrt[6]{2}, \zeta) = \mathbb{Q}(\sqrt[6]{2}, \zeta\sqrt[6]{2}, \dots, \zeta^{p-1}\sqrt[6]{2}$ da $\zeta = (\zeta\sqrt[6]{2})/\sqrt[6]{2}$. Somit wird L von den Nullstellen von f erzeugt, ist also ein Zerfällungskörper vor f.

2. Das Polynom f ist separabel, da alle Nullstellen paarweise verschieden sind. Somit ist L als Zerfällungskörper des separablen Polynoms $f \in \mathbb{Q}[X]$ galoisch über $\mathbb{Q}$.

3. Als p-te Einheitswurzel ist ζ eine Nullstelle des Polynoms $X^p - 1 \in \mathbb{Q}[X]$. Dabei gilt $X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \cdots + X + 1)$, und da $\zeta \neq 1$ gilt, erhalten wir, dass ζ bereits eine Nullstelle von $g(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Q}[X]$ ist. Durch Eisenstein bezüglich der Primzahl p ergibt sich, dass das Polynom $g(X+1)$ irreduzibel ist; somit ist auch g irreduzibel (man siehe Übung 35 und die zugehörigen Lösungen für eine detailiertere Rechnung). Also ist g bereits das Minimalpolynom von ζ, und somit $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg g = p - 1$.

4. Das Minimalpolynom von $\sqrt[p]{2}$ über $\mathbb{Q}$ ist $X^p - 2 \in \mathbb{Q}[X]$, da dieses Polynom nach Eisenstein irreduzibel ist. Deshalb gilt $[\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] = \deg(X^p - 2) = p$. Außerdem gilt $[L : \mathbb{Q}(\sqrt[p]{2})] \leq p - 1$, da $L = \mathbb{Q}(\sqrt[p]{2})(\zeta)$ gilt und ζ eine Nullstelle von $g(X) \in \mathbb{Q}(\sqrt[p]{2})[X]$ ist. Somit gilt insgesamt

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[p]{2})][\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] \leq p(p-1).$$

   Andererseits gilt $\mathbb{Q}(\sqrt[p]{2}) \subseteq L$ und somit $p = [\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] \mid [L : \mathbb{Q}]$, sowie analog auch $\mathbb{Q}(\zeta) \subseteq L$ und somit $p-1 = [\mathbb{Q}(\zeta) : \mathbb{Q}] \mid [L : \mathbb{Q}]$. Da p prim ist sind p und $p-1$ teilerfremd; also gilt bereits $p(p-1) \mid [L : \mathbb{Q}]$ und somit auch $p(p-1) \leq [L : \mathbb{Q}]$.

5. Da $L/\mathbb{Q}$ galoisch ist, wissen wir bereits, dass $|\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = p(p-1)$ gilt. Jedes $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ permutiert die Nullstellen von f, weshalb $\sigma(\sqrt[p]{2}) = \zeta^k \sqrt[p]{2}$ für ein eindeutiges $k \in \{0, \ldots, p-1\}$ gilt. Außerdem muss σ die Nullstellen von g, also die p-ten Einheitswurzeln, die verschieden von 1 sind, permutieren, weshalb $\sigma(\zeta) = \zeta^\ell$ für ein eindeutiges $\ell \in \{1, \ldots, p-1\}$ gilt. Da σ durch die beiden Werte $\sigma(\sqrt[p]{2})$ und $\sigma(\zeta)$ bereits eindeutig bestimmt ist, erhalten wir zusammen mit $|\mathrm{Gal}(L/\mathbb{Q})| = p(p-1)$, dass $\mathrm{Gal}(L/\mathbb{Q}) = \{\sigma_{k,\ell} \mid k = 0, \ldots, p-1; \ell = 1, \ldots, p-1\}$ gilt, wobei $\sigma_{k,\ell}$ durch

$$\sigma_{k,\ell} \colon \begin{cases} \sqrt[p]{2} & \mapsto & \zeta \sqrt[p]{2}, \\ \zeta & \mapsto & \zeta^\ell, \end{cases}$$

   eindeutig bestimmt ist. (Wir wählen die Indizes so, dass man sich den Parameter k als ein Element von $\mathbb{Z}/p$ vorstellen kann, und den Parameter ℓ als ein Element von $(\mathbb{Z}/p)^\times$.)

6. Für $p = 2$ gilt $|\mathrm{Gal}(L/\mathbb{Q})| = 2$ und $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2$ ist abelsch. Für $p \neq 3$ Gruppe ist nicht abelsch, denn dann gilt $\sigma_{1,1}\sigma_{0,2} \neq \sigma_{0,2}\sigma_{1,1}$ da

$$\sigma_{1,1}(\sigma_{0,2}(\sqrt[p]{2})) = \sigma_{1,1}(\sqrt[p]{2}) = \zeta \sqrt[p]{2} \neq \zeta^2 \sqrt[p]{2} = \sigma_{0,2}(\zeta \sqrt[p]{2}) = \sigma_{0,2}(\sigma_{1,1}(\sqrt[p]{2})).$$

7. Für $p = 2$ ist $\mathrm{Gal}(L/\mathbb{Q})$ abelsch und somit jede Untergruppe normal. Wir betrachten daher im Folgenden nur den Fall $p \neq 2$. Die Untergruppe

$$H \coloneqq \mathrm{Gal}(L/\mathbb{Q}(\sqrt[p]{2})) = \{\sigma_{0,1}, \ldots, \sigma_{0,p-1}\}$$

   ist dann nicht normal in $\mathrm{Gal}(L/\mathbb{Q})$. Es gibt (mindestens) zwei Möglichkeiten dies einzusehen:

- Es gilt $\sigma_{1,1}^{-1} = \sigma_{p-1,1}$ denn es gelten

$$\begin{aligned}\sigma_{1,1}(\sigma_{p-1,1}(\sqrt[p]{2})) = \sigma_{1,1}(\zeta^{p-1}\sqrt[p]{2}) &= \sigma_{1,1}(\zeta)^{p-1}\sigma_{1,1}(\sqrt[p]{2}) \\ &= \zeta^{p-1}\zeta\sqrt[p]{2} = \zeta^p\sqrt[p]{2} = \sqrt[p]{2}\end{aligned}$$

  sowie $\sigma_{1,1}(\sigma_{p-1,1}(\zeta)) = \sigma_{1,1}(\zeta) = \zeta$, und somit $\sigma_{1,1}\sigma_{p-1,1} = \mathrm{id}_L$. Für $\sigma_{0,2} \in H$ gilt somit $\sigma_{1,1}\sigma_{0,2}\sigma_{1,1}^{-1} = \sigma_{1,1}\sigma_{0,2}\sigma_{p-1,1} = \sigma_{p-1,2} \notin H$, denn

$$\begin{aligned}\sigma_{1,1}(\sigma_{0,2}(\sigma_{p-1,1}(\sqrt[p]{2}))) &= \sigma_{1,1}(\sigma_{0,2}(\zeta^{p-1}\sqrt[p]{2})) = \sigma_{1,1}(\sigma_{0,2}(\zeta)^{p-1}\sigma_{0,2}(\sqrt[p]{2})) \\ &= \sigma_{1,1}((((\zeta)^2)^{p-1}\sqrt[p]{2}) = \sigma_{1,1}(\zeta^{2p-2}\sqrt[p]{2}) \\ &= \sigma_{1,1}(\zeta)^{2p-2}\sigma_{1,1}(\sqrt[p]{2}) = \zeta^{2p-2}\zeta\sqrt[p]{2} \\ &= \zeta^{2p-1}\sqrt[p]{2} = \zeta^{p-1}\sqrt[p]{2}\end{aligned}$$

  sowie

$$\sigma_{1,1}(\sigma_{0,2}(\sigma_{p-1,1}(\zeta))) = \sigma_{1,1}(\sigma_{0,2}(\zeta)) = \sigma_{1,1}(\zeta^2) = \sigma_{1,1}(\zeta)^2 = \zeta^2.$$

- Wäre H normal in G, so wäre nach dem Hauptsatz der Galoistheorie die Erweiterung $\mathbb{Q}(\sqrt[p]{2})/\mathbb{Q}$ galoisch. Die Erweiterung ist aber nicht normal, denn f ist irreduzibel in $\mathbb{Q}[X]$ und hat eine Nullstelle in $\mathbb{Q}(\sqrt[p]{2})$, zerfällt aber in $\mathbb{Q}(\sqrt[p]{2})[X]$ nicht in Linearfaktoren, denn die weiteren Nullstellen $\zeta\sqrt[p]{2}, \ldots, \zeta^{p-1}\sqrt[p]{2}$ von f liegen nicht in $\mathbb{R}$ und somit auch nicht in $\mathbb{Q}(\sqrt[p]{2})$.

8. Die Gruppe

$$N \coloneqq \mathrm{Gal}(L/\mathbb{Q}(\zeta)) = \{\sigma_{0,1}, \ldots, \sigma_{p-1,1}\}$$

   ist normal in $\mathrm{Gal}(L/\mathbb{Q})$. Es gibt (mindestens) zwei Möglichkeiten dies einzusehen:

   - Man bemerke, dass für alle $\sigma_{k,\ell}, \sigma_{k',\ell'} \in \mathrm{Gal}(L/\mathbb{Q})$ die Gleichheit

$$\sigma_{k,\ell}(\sigma_{k',\ell'}(\zeta)) = \sigma_{k,\ell}(\zeta)^{\ell'} = ((\zeta)^{\ell})^{\ell'} = \zeta^{\ell\ell'} = \zeta^{\ell'\ell} = \cdots = \sigma_{k',\ell'}(\sigma_{k,\ell}(\zeta))$$

     gilt. Obwohl $\mathrm{Gal}(L/\mathbb{Q})$ für $p \neq 2$ nicht abelsch ist, lassen sich die Gruppenelemente beim Auswerten an ζ deshalb dennoch vertauschen. Für $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ und $\sigma' \in N$ gilt deshalb auch $\sigma\sigma'\sigma^{-1} \in N$, denn es gilt

$$\sigma(\sigma'(\sigma^{-1}(\zeta))) = \sigma(\sigma^{-1}(\sigma'(\zeta))) = \sigma'(\zeta) = \zeta.$$

   - Nach dem Hauptsatz der Galoistheorie ist N genau dann normal in $\mathrm{Gal}(L/\mathbb{Q})$, wenn $\mathbb{Q}(\zeta)/\mathbb{Q}$ galoisch ist. Hierfür bemerke man, dass $\mathbb{Q}(\zeta)$ alle Potenzen ζ^k enthält, also alle p-ten Einheitswurzeln (denn ζ ist eine *primitive* p-te Einheitswurzel). Also ist $\mathbb{Q}(\zeta)$ der Zerfällungskörper des Kreisteilungspolynoms $X^p - 1 \in \mathbb{Q}[X]$; dieses ist separabel, da die p-ten Einheitswurzeln paarweise verschieden sind. Somit ist $\mathbb{Q}(\zeta)$ der Zerfällungskörper eines separablen Polynoms aus $\mathbb{Q}[X]$, und $\mathbb{Q}(\zeta)/\mathbb{Q}$ somit galoisch.

Bemerkung. Für die Untergruppen $N, H \subseteq \mathrm{Gal}(L/\mathbb{Q})$ ist also N normal und $H \cap N = 1$. Es gilt außerdem $NH = G$, da $\sigma_{k,\ell} = \sigma_{k,1}\sigma_{1,\ell}$ für alle k, ℓ gilt, wobei $\sigma_{k,1} \in N$ und $\sigma_{0,\ell} \in N$ gelten. Insgesamt erhält man hierdurch, dass $\mathrm{Gal}(L/\mathbb{Q}) = N \rtimes H$. Zusammen mit $N \cong \mathbb{Z}/p$ und $H \cong (\mathbb{Z}/p)^\times$ erhält man somit, dass $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/p) \rtimes (\mathbb{Z}/p)^\times$ gilt.

Für $p = 2$ ergibt sich somit, dass $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2$, und für $p = 3$ ergibt sich, dass $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/3) \rtimes (\mathbb{Z}/2) \cong S_3$.

Lösung 92.

(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 gilt $0 \neq K$, 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.

Lösung 93.

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.

Lösung 94.

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

Lösung 95.

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 $n = \deg P$. Es gilt also

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

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

Lösung 96.

1. Wegen der algebraischen Abgeschlossenheit von $\overline{L}$ ist $\overline{L}/K$ genau dann ein algebraischer Abschluss, wenn $\overline{L}/K$ algebraisch ist. Da $\overline{L}/L$ algebraisch ist folgt aus der Transitivität von Algebraizität, dass dies genau dann gilt, wenn L/K algebraisch ist.

2. Es sei $\overline{K} \coloneqq \{x \in \overline{L} \mid x \text{ is algebraisch über } K\}$. Dann ist $K \subseteq \overline{K} \subseteq \overline{L}$ ein Zwischenkörper, so dass $\overline{K}/K$ algebraisch ist. Jedes nicht-konstante Polynom $f \in \overline{K}[X] \subseteq \overline{L}[X]$ hat eine Nullstelle $x \in \overline{L}$, da $\overline{L}$ algebraisch abgeschlossen ist. Dann ist x algebraisch über $\overline{K}$, und wegen der Transitivität von Algebraizität damit auch algebraisch über K; somit gilt bereits $x \in \overline{K}$. Das zeigt, dass $\overline{K}$ algebraisch abgeschlossen ist.

3. Es sei $K \subseteq \overline{K}' \subseteq \overline{L}$ ein weiterer Zwischenkörper, so dass $\overline{K}'/K$ ein algebraischer Abschluss ist. Dann ist $\overline{K}'/K$ algebraisch und somit $\overline{K}' \subseteq \overline{K}$. Wir haben also einen Erweiterungsturm $\overline{K}/\overline{K}'/K$. Da $\overline{K}/K$ algebraisch ist, ist es auch $\overline{K}/\overline{K}'$; da $\overline{K}'$ algebraisch abgeschlossen ist, gilt deshalb bereits $\overline{K} = \overline{K}'$ (siehe Übung 95).

Lösung 97.
Es sei L/K eine endliche Körpererweiterung und $x \in L$. Für den K-Untervektorraum $\langle\{x^n \mid n \in \mathbb{N}\}\rangle_K \subseteq L$ gilt

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

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

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

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

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

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

Lösung 98.
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 $a_0, \ldots, a_n \in L$ die Koeffizienten von p. Da L/K algebraisch ist sind $a_0, \ldots, a_n$ algebraisch über K. Für $L' \coloneqq K(a_0, \ldots, a_n)$ 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 97). Inbesondere ist x algebraisch über K.

Lösung 99.
Sind α und β algebraisch über K, so ist $K(\alpha, \beta)/K$ eine algebraische Körpererweiterung. Da $\alpha + \beta, \alpha\beta \in K(\alpha, \beta)$ gilt, 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

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

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

Lösung 100.

1. Wegen der Irreduziblität von f gilt $\deg f \geq 1$. Wegen $\operatorname{char} K = 0$ folgt, dass $f' \neq 0$. Da aber $\deg f' = \deg f - 1 < \deg f$ gilt, folgt aus der Irreduziblität von f, dass f und f' teilerfremd sind. Also ist f separabel.

2. Ist $p \coloneqq \operatorname{char} K > 0$, so ist das Polynom $f(X) \coloneqq X^p - t \in \mathbb{F}_p(t)[X]$ nach Eisenstein irreduzibel. Es gilt aber $f' = 0$, weshalb f und f' nicht teilerfremd, und f somit nicht separabel ist.

Lösung 101.

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 die beiden Erweiterungen L_1/K und L_2/K. Deshalb gelten $L_1 = K(\alpha_1, \ldots, \alpha_n)$ 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 $[L_1 L_2 : K] = [L_1 : K][L_2 : K]$.

Lösung 102.

1. Ist $\alpha \in L$ mit $\alpha \notin K$, 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 $c \in K$ wegen der Irreduziblität von f kein Quadrat ist.

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

2. Es sei $\alpha \in L$ mit $\alpha \notin K$ und $\alpha^2 \in K$. Dann ist $f(X) \coloneqq X^2 - \alpha^2 \in K[X]$ 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 $|\operatorname{Gal}(L/K)| = 2 = [L : K]$ gilt:
     - Jedes $\sigma \in \operatorname{Gal}(L/K)$ 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 $\operatorname{Gal}(L/K) = \{\mathrm{id}_L, \tau\}$.
     - Es gilt $2 \leq |\operatorname{Gal}(L/K)| \leq [L : K] = 2$.
   - 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 $L \coloneqq K[X]/(f)$ ist dann $\overline{X} \in L$ nicht separabel, da f das Minimalpolynom von $\overline{X}$ ist. Somit ist L/K auch nicht galoisch.

Lösung 103.

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

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 (siehe Übung 96). 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 auch $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = 2$.

   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 102) und damit insbesondere normal. Die Erweiterung $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ ist allerdings nicht normal, denn das Polynom $f(X) \coloneqq X^4 - 2 \in \mathbb{Q}[X]$ 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 $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$).

Lösung 104.

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 K 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.

Lösung 105.

Wir geben zwei mögliche Lösungen an:

- Nach dem Hauptsatz der Galoistheorie ist E/K genau dann Galoisch, wenn die Untergruppe $\operatorname{Gal}(L/E) \subseteq \operatorname{Gal}(L/K)$ normal ist.

  Es gelte zunächst $\sigma(E) = E$ für alle $\sigma \in \operatorname{Gal}(L/K)$, und es seien $\sigma \in \operatorname{Gal}(L/K)$ und $\tau \in \operatorname{Gal}(L/E)$. Für jedes $e \in E$ gilt nach Annahme $\sigma^{-1}(e) \in E$, also $\tau(\sigma^{-1}(e)) = \sigma^{-1}(e)$

und somit $\sigma(\tau(\sigma^{-1}(e))) = \sigma(\sigma^{-1}(e)) = e$. Also gilt $\sigma\tau\sigma^{-1} \in \mathrm{Gal}(L/E)$. Das zeigt, dass $\mathrm{Gal}(L/E)$ normal in $\mathrm{Gal}(L/E)$ ist.

Es sei nun $\mathrm{Gal}(L/E)$ normal in $\mathrm{Gal}(L/K)$, und es sei $\sigma \in \mathrm{Gal}(L/K)$. Nach Annahme gilt $\mathrm{Gal}(L/E)\sigma = \sigma\,\mathrm{Gal}(L/E)$, weshalb es für jedes $\tau \in \mathrm{Gal}(L/E)$ ein $\tau' \in \mathrm{Gal}(L/E)$ mit $\tau\sigma = \sigma\tau'$ gibt. Für jedes $e \in E$ gilt deshalb, dass

$$\tau(\sigma(e)) = \sigma(\tau'(e)) = \sigma(e) \qquad \text{für alle } \tau \in \mathrm{Gal}(L/E)$$

gilt. Also gilt $\sigma(e) \in L^{\mathrm{Gal}(L/E)}$ für alle $e \in E$; nach dem Hauptsatz der Galoistheorie gilt $L^{\mathrm{Gal}(L/E)} = E$, weshalb $\sigma(E) \subseteq E$.

Für alle $\sigma \in \mathrm{Gal}(L/K)$ gilt also $\sigma(E) \subseteq E$. Da dies auch für σ^{-1} gilt, erhalten wir mit $\sigma^{-1}(E) \subseteq E$, dass $E = \sigma(\sigma^{-1}(E)) \subseteq \sigma(E) \subseteq E$ und somit $E = \sigma(E)$ gilt.

- Die Erweiterung L/K ist separabel und normal, da sie Galoisch ist. Damit ist auch L/E separabel; es bleibt also nur zu zeigen, dass E/K genau dann normal ist, wenn $\sigma(E) = E$ für alle $\sigma \in \mathrm{Gal}(L/K)$ gilt.

  Da L/K algebraisch ist gibt es einen algebraischen Abschluss $\overline{K}$ von K, der L enthält (siehe Übung 96).

  Es sei zunächst E/K normal und $\sigma \in \mathrm{Gal}(L/K)$. Es seien $\iota_E\colon E \to \overline{K}$, $x \mapsto x$ und $\iota_L\colon L \to \overline{K}$, $x \mapsto x$ die kanonische Inklusionen. Es sei außerdem $\iota_{LE}\colon E \to L$, $x \mapsto x$ die kanonische Inklusion; es gilt $\iota_E = \iota_L\iota_{LE}$.

  Es sind $\iota_E\colon E \to \overline{K}$ und $\iota_L \circ \sigma \circ \iota_{LE}\colon E \to \overline{K}$ zwei K-lineare Körperhomomorphismen. Da E/K normal ist haben sie das gleiche Bild; es gilt also

  $$E = \iota_E(E) = \iota_L(\sigma(\iota_{LE}(E))) = \sigma(E).$$

  Es gelte nun $\sigma(E) = E$ für alle $\sigma \in \mathrm{Gal}(L/K)$. Es sei $\varphi\colon E \to \overline{K}$ ein K-linearer Körperhomomorphismus. Da L/E algebraisch ist, lässt sich φ zu einem Körperhomomorphismus $\psi\colon L \to \overline{K}$ fortsetzen; da $\psi|_K = \varphi|_K = \mathrm{id}_K$ gilt, ist auch ψ K-linear. Da L/K normal ist und $\overline{K}$ ein algebraischer Abschluss von K ist, gilt $\psi(L) = L$ (denn auch $\iota\colon L \to \overline{K}$, $x \mapsto x$ ist eine K-lineare Einbettung, und wegen der Normalität von L/K gilt bereits $\operatorname{im}\psi = \operatorname{im}\iota = L$). Also schränkt sich ψ zu einem K-linearen Automorphismus $\sigma\colon L \to L$, $x \mapsto \psi(x)$ ein. Nach Annahme gilt somit

  $$E = \sigma(E) = \psi(E) = \varphi(E) = \operatorname{im}\varphi.$$

  Das Bild von φ hängt also nicht von φ selbst ab; dies zeigt die Normalität von E/K.

Lösung 106.

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 117). Jede abelsche Gruppe trägt eine eindeutige $\mathbb{Z}$-Modulstruktur (siehe Übung 116), 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: Es gibt eine kurze exakte Sequenz $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ von $\mathbb{Z}$-Moduln. Dabei ist $\mathbb{Z}$ endlich erzeugt; wäre $\mathbb{Q}/\mathbb{Z}$ endlich erzeugt, so wäre dies deshalb auch $\mathbb{Q}$ (siehe Übung 125), was aber nicht gilt (siehe Übung 113).

3. Die Aussage ist wahr: Ist $f\colon \mathbb{Z}/2 \to \mathbb{Z}/3$ ein Homomorphismus von $\mathbb{Z}$-Moduln, so ist $2 \cdot f(\overline{1}) = f(\overline{2}) = f(\overline{0}) = \overline{0}$. Das einzige Element aus $\mathbb{Z}/3$, was für $f(\overline{1})$ in Frage kommt, ist deshalb $\overline{0}$. Also muss $f(\overline{1}) = \overline{0}$ und somit $f = 0$.

4. 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 $K[X]/(X-b)$ deshalb nicht isomorph.
   - Wäre $K[X]/(X-a) \cong K[X]/(X-b)$ als $K[X]$-Moduln, so wäre nach Übung 134 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:

$$\begin{array}{ccc} K[X]/(X-a) & \xrightarrow{X\cdot} & K[X]/(X-a) \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi} \\ K[X]/(X-b) & \xrightarrow{X\cdot} & K[X]/(X-b) \end{array}$$

     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:

$$\begin{array}{ccc} K[X]/(X-a) & \xrightarrow{a\cdot} & K[X]/(X-a) \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi} \\ K[X]/(X-b) & \xrightarrow{b\cdot} & K[X]/(X-b) \end{array}$$

     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 $a = b$.

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

6. Die Aussage ist falsch:
   - Betrachtet man $R = \mathbb{Z}/6$, so gibt es eine Zerlegung $\mathbb{Z}/6 = \mathbb{Z}/2 \oplus \mathbb{Z}/3$ von $\mathbb{Z}$-Moduln, und damit auch von $\mathbb{Z}/6$-Moduln. Die beiden $\mathbb{Z}/6$-Moduln $\mathbb{Z}/2$ und $\mathbb{Z}/3$ sind aber nicht frei da $2, 3 \neq 6^n$ für alle $n \geq 0$ gilt.

- 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 58) 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 Spann eines Basiselements, und J als den Spann 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 $I \oplus J$.

7. 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.

8. 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 $P \cap N \neq 0$.

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

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

als R-Moduln.

10. 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 58). 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.

11. 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.

12. Die Aussage ist wahr: Da M ein endliches Erzeugendensystem besitzt, enthält jedes Erzeugendensystem $E \subseteq M$ bereits ein endliches Erzeugendensystem $E' \subseteq E$ (siehe Übung 120). Ist E bereits minimal, so muss dabei $E = E'$ gelten, und E somit bereits endlich sein.

13. 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.

14. 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 $s \colon \mathbb{Z} \oplus \bigoplus_{n \geq 2} (\mathbb{Z}/2) \to \mathbb{Z}$ 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.

15. 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 123).

16. Die Aussage ist wahr: Es gibt einen surjektiven Modulhomomorphismus $\varphi\colon F \to P$ für einen freien R-Modul F (siehe Übung 118). 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 123 für die verschiedenen Charakterisierungen projektiver Moduln.)

17. Die Aussage ist falsch: Man siehe Übung 136 für ein Gegenbeispiel.

18. Die Aussage ist falsch: Man betrachten für $R \neq 0$ den R-Modul $M = \bigoplus_{n\in\mathbb{N}} R$.

Lösung 107.

1. Der Hauptsatz besagt, dass für einen Hauptidealring R jeder endliche erzeugte R-Modul M von der Form

$$M \cong R^s \oplus \bigoplus_{p\in\mathcal{P}} \bigoplus_{i=1}^{r_p} R/(p^{\nu(p,i)})$$

ist, wobei $\mathcal{P}$ ein Repräsentantensystem der Primelemente von R ist und die Exponenten $\nu(p,1),\dots,\nu(p,r_p)$ positive natürliche Zahlen sind. Dabei sind die Zahlen r_p für $p \in \mathcal{P}$ eindeutig, und für jedes $p \in \mathcal{P}$ sind die Zahlen $r_1,\dots,r_p$ eindeutig bis auf Permutation. (Fordert man zusätzlich, dass $r_1 \leq \cdots \leq r_p$ gelte, so werden die Zahlen eindeutig.)

2. Es sei K ein algebraisch abgeschlossener Körper und $f\colon V \to V$ ein Endomorphismus eines endlichdimensionalen K-Vektorraums V. Dann lässt sich die K-Vektorraumstruktur von V eindeutig zu einer $K[T]$-Modulstruktur erweitern, so dass $T\cdot v = f(v)$ für alle $v \in V$ gilt. Der Ring $K[T]$ ist ein Hauptidealring, da K ein Körper ist; da K algebraisch abgeschlossen ist, bildet die Menge der Linearfaktoren $\mathcal{P} = \{T-\lambda \mid \lambda \in K\}$ ein Repräsentantensystem der Primelemente von $K[T]$. Nach dem obigen Hauptsatz gibt es eine Zerlegung

$$\begin{aligned} V &\cong K[T]^s \oplus \bigoplus_{p\in\mathcal{P}} \bigoplus_{i=1}^{r_p} K[T]/(p^{\nu(p,i)}) \\ &= K[T]^s \oplus \bigoplus_{\lambda\in K} \bigoplus_{i=1}^{r_{T-\lambda}} K[T]/((T-\lambda)^{\nu(T-\lambda,i)}) \\ &= K[T]^s \oplus \bigoplus_{\lambda\in K} \bigoplus_{i=1}^{s_\lambda} K[T]/((T-\lambda)^{\mu(\lambda,i)}). \end{aligned}$$

für $s_\lambda \coloneqq r_{T-\lambda}$ und $\mu(\lambda, i) = \nu(T - \lambda, i)$. Dies ist inbesondere eine Isomorphie von K-Vektorräumen. Wegen der Endlichdimensionalität von V gilt somit $s = 0$, und deshalb bereits

$$V \cong \bigoplus_{\lambda \in K} \bigoplus_{i=1}^{s_\lambda} K[T]/((T-\lambda)^{\mu(\lambda,i)}).$$

Die Summanden $K[T]/((T-\lambda)^{\mu(\lambda,i)})$ entsprechen dabei f-invarianten Untervektorräumen von V. Um die Existenz einer Jordanbasis von V bezüglich f zu zeigen, genügt es daher zu zeigen, dass es für alle $\lambda \in K$ und $n \geq 0$ eine K-Basis $\mathcal{B} = (x_1, \ldots, x_n)$ von $K[T]/((T-\lambda)^n)$ gibt, so dass der K-lineare Endomorphismus

$$\tilde{f} \colon K[T]/((T-\lambda)^n) \to K[T]/((T-\lambda)^n), \quad x \mapsto T \cdot x$$

bezüglich $\mathcal{B}$ durch einen Jordanblock zum Eigenwert λ dargestellt wird, also

$$\mathrm{Mat}_{\mathcal{B}}(\tilde{f}) = \begin{pmatrix} \lambda & 1 & & & & \\ & \lambda & 1 & & & \\ & & \ddots & \ddots & & \\ & & & \ddots & 1 & \\ & & & & \lambda & 1 \\ & & & & & \lambda \end{pmatrix}$$

gilt. Eine solche Basis ist durch

$$\mathcal{B} = \left(\overline{(T-\lambda)}^{n-1}, \overline{(T-\lambda)}^{n-2}, \ldots, \overline{T-\lambda}, \overline{1}\right)$$

gegeben, denn für alle $i \geq 0$ gilt

$$\begin{aligned} \tilde{f}\left(\overline{(T-\lambda)}^{i}\right) &= T \cdot \overline{(T-\lambda)}^{i} \\ &= (T-\lambda) \cdot \overline{(T-\lambda)}^{i} + \lambda \overline{(T-\lambda)}^{i} = \overline{(T-\lambda)}^{i+1} + \lambda \overline{(T-\lambda)}^{i}, \end{aligned}$$

wobei $\overline{(T-\lambda)}^{i+1} = 0$ für alle $i \geq n-1$ gilt.

Lösung 108.

1. Es gilt $213 = 3 \cdot 71$. Nach dem Hauptsatz über endlich erzeugt abelsche Gruppen ist $\mathbb{Z}/3 \oplus \mathbb{Z}/71$ bis auf Isomorphie die einzige abelsche Gruppe von Ordnung 213.
2. Es gilt $675 = 3^3 \cdot 5^2$. Nach dem Hauptsatz über endlich erzeugt abelsche Gruppen gibt es bis auf Isomorphie 6 abelsche Gruppen der Ordnung 675, und diese sind

$$\begin{aligned} &\mathbb{Z}/27 \oplus \mathbb{Z}/25, \\ &\mathbb{Z}/27 \oplus \mathbb{Z}/5 \oplus \mathbb{Z}/5, \\ &\mathbb{Z}/9 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/25, \\ &\mathbb{Z}/9 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/5 \oplus \mathbb{Z}/5, \\ &\mathbb{Z}/3 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/25, \\ &\mathbb{Z}/3 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/5 \oplus \mathbb{Z}/5. \end{aligned}$$

3. Es gilt $3087 = 3^2 \cdot 7^3$. Nach dem Hauptsatz über endlich erzeugt abelsche Gruppen gibt es bis auf Isomorphie 6 abelsche Gruppen der Ordnung 3087, und diese sind

$$\begin{aligned}
&\mathbb{Z}/9 \oplus \mathbb{Z}/343,\\
&\mathbb{Z}/3 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/343,\\
&\mathbb{Z}/9 \oplus \mathbb{Z}/49 \oplus \mathbb{Z}/7,\\
&\mathbb{Z}/3 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/49 \oplus \mathbb{Z}/7,\\
&\mathbb{Z}/9 \oplus \mathbb{Z}/7 \oplus \mathbb{Z}/7 \oplus \mathbb{Z}/7,\\
&\mathbb{Z}/3 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/7 \oplus \mathbb{Z}/7 \oplus \mathbb{Z}/7.
\end{aligned}$$

4. Es gilt $152460 = 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11^2$. Nach dem Hauptsatz über endlich erzeugt abelsche Gruppen gibt es bis auf Isomorphie 8 abelsche Gruppen der Ordnung 3087, und diese sind

$$\begin{aligned}
&\mathbb{Z}/4 \oplus \mathbb{Z}/9 \oplus \mathbb{Z}/5 \oplus \mathbb{Z}/7 \oplus \mathbb{Z}/121,\\
&\mathbb{Z}/4 \oplus \mathbb{Z}/9 \oplus \mathbb{Z}/5 \oplus \mathbb{Z}/7 \oplus \mathbb{Z}/11 \oplus \mathbb{Z}/11,\\
&\mathbb{Z}/4 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/5 \oplus \mathbb{Z}/7 \oplus \mathbb{Z}/121,\\
&\mathbb{Z}/4 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/5 \oplus \mathbb{Z}/7 \oplus \mathbb{Z}/11 \oplus \mathbb{Z}/11,\\
&\mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/9 \oplus \mathbb{Z}/5 \oplus \mathbb{Z}/7 \oplus \mathbb{Z}/121,\\
&\mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/9 \oplus \mathbb{Z}/5 \oplus \mathbb{Z}/7 \oplus \mathbb{Z}/11 \oplus \mathbb{Z}/11,\\
&\mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/5 \oplus \mathbb{Z}/7 \oplus \mathbb{Z}/121,\\
&\mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/5 \oplus \mathbb{Z}/7 \oplus \mathbb{Z}/11 \oplus \mathbb{Z}/11.
\end{aligned}$$

Lösung 109.

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

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

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

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 $7M_4 \cong \mathbb{Z}/4$ 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

$$M_6 \cong \mathbb{Z}/3 \oplus \mathbb{Z}/21 \cong \mathbb{Z}/3 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/7.$$

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

b) Eine Smith-Normalform ist $A_9' = \left(\begin{smallmatrix} 1 & 0 \\ 0 & t^2 - t \end{smallmatrix}\right)$. Deshalb gilt

$$M_9 \cong \mathbb{Q}[t]/(t^2 - t) \cong \mathbb{Q}[t]/(t) \oplus \mathbb{Q}[t]/(t-1).$$

Inbesondere ist M_9 ein Torsionsmodul, und es gilt $M_9 = (t-1)M_9 \oplus tM_9$, wobei $(t-1)M_9 \cong \mathbb{Q}[t]/(t)$ der t-primäre Anteil von M_9 ist, und $tM_9 \cong \mathbb{Q}[t]/(t-1)$ der $(t-1)$-primäre Anteil.

Lösung 110.
Es sei $\mathcal{P} = \{2, 3, 5, 7, 11, \dots\}$ die Menge der 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

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

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

Lösung 111.
Wir zeigen, dass die Abbildung $\varphi\colon \operatorname{Hom}_R(R, M) \to M$, $f \mapsto f(1)$ ein Isomorphismus von R-Moduln ist: Dass φ ein Homomorphismus von R-Moduln ist, ergibt sich direkt daraus, dass die R-Modulstruktur auf $\operatorname{Hom}_R(R, M)$ 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 den Funktionswert $f(1)$ bereits eindeutig bestimmt ist. Für jedes $m \in M$ ist $f_m\colon R \to M$, $r \mapsto rm$ ein Homomorphismus von R-Moduln. Es gilt $\varphi(f_m) = f_m(1) = m$, was die Surjektivität von φ zeigt.

Lösung 112.
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 es gilt $2 \cdot \mathbb{Z}/2 = 0$.
   - $\mathbb{Z}/2$ wäre isomorph zu einer Untergruppe von $\mathbb{Z}$, und müsste somit entweder trivial oder unendlich sein, was beides nicht gilt.

2. Es gibt zwei mögliche Argumentationsweisen: Die erste ist recht direkt:

   - 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.

   Die zweite nutzt die Äquivalenz der verschiedenen Charakterisierungen projektiver Moduln (siehe Übung 123), in deren Beweis sich die obige Rechnung versteckt.

   - Als freier R-Modul ist F insbesondere projektiv, da $F \oplus 0 \cong F$ frei ist. Somit spaltet jede kurze exakte Sequenz von R-Moduln, die in F endet.

Lösung 113.
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

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

  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 $\mathbb{Z}$ als Hauptidealring insbesondere noethersch ist, wäre $\mathbb{Q}$ als endlich erzeugter $\mathbb{Z}$-Modul bereits noethersch (siehe Übung 127). Dann würde jede aufsteigende Kette von $\mathbb{Z}$-Untermoduln von $\mathbb{Q}$ stabilisieren (siehe Übung 126). Die Kette

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

  stabilisiert aber nicht.

Lösung 114.
Da M noethersch ist stabilisiert die Kette

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

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, dass $\ker f^n = 0$ gilt, und wegen $\ker f \subseteq \ker f^n$ somit auch $\ker f = 0$. Also ist f injektiv, und somit bereits ein Isomorphismus.

Lösung 115.

1. Ist M einfach, so muss $M \neq 0$ gelten, 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.

Lösung 116.

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

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

bekannt. Dabei ist

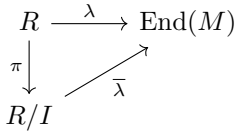
$$\operatorname{End}(A) = \{f\colon A \to A \mid f \text{ ist additiv}\}$$

ein Ring unter punktweiser Adddition und Komposition. Da es genau einen Ringhomomorphismus $\mathbb{Z} \to \operatorname{End}(A)$ gibt (siehe Übung 48) folgt die Aussage.

Lösung 117.

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

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

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

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

$$\begin{array}{ccc} R_S & & \\ {\scriptstyle i}\uparrow & \searrow^{\hat{\lambda}} & \\ R & \xrightarrow{\lambda} & \mathrm{End}(M) \end{array}$$

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.

Lösung 118.

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 $\varphi(x) \coloneqq \sum_{i\in I} r_i m_i$ wohldefiniert, und liefert eine Funktion $\varphi\colon F \to M$. Ist $r \in R$ und sind $x, y \in F$ mit $x = \sum_{i\in I} r_i b_i$ und $y = \sum_{i\in I} s_i b_i$, so gelten $rx = \sum_{i\in I} r r_i b_i$ und $x + y = \sum_{i\in I}(r_i + s_i) b_i$. Deshalb gilt

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

und

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

Also ist φ ein Modulhomomorphismus.

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 $\overline{\varphi}\colon F/\ker\varphi \to M$, $x \mapsto \varphi(x)$.

Lösung 119.
(1 $\implies$ 2) Es sei $m \in M$ mit $M = \langle m \rangle_R$. Dann gilt

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

(siehe Übung 135). Für den surjektive Homomorphismus von R-Moduln $\varphi\colon R \to M$, $r \mapsto rm$ gilt deshalb $\ker \varphi = \operatorname{Ann}(M)$. Somit induziert φ einen Isomorphismus von R-Moduln

$$\bar{\varphi}\colon R/\operatorname{Ann}(M) \to M, \quad \overline{r} \mapsto rm.$$

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

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

Lösung 120.
Es sei $\{m_1, \ldots, m_s\} \subseteq M$ ein endliches Erzeugendensystem. Da E ein Erzeugendensystem ist, lässt sich jedes m_i als $m_i = r_{i,1}e_{i,1} + \cdots + r_{i,t_i}e_{i,t_i}$ mit $t_i \geq 0$, $e_{i,1}, \ldots, e_{i,t_i} \in E$ und $r_{i,1}, \ldots, r_{i,t_i} \in R$ schreiben. Für $E' \coloneqq \{e_{i,j} \mid i = 1, \ldots, s, j = 1, \ldots, t_i\}$ gilt dann $m_i \in \langle E' \rangle$ für alle $i = 1, \ldots, s$, und somit

$$M = \langle m_1, \ldots, m_s \rangle \subseteq \langle E' \rangle \subseteq M.$$

Also gilt $\langle E' \rangle = M$, weshalb E' ein endliches Erzeugendensystem von M ist.

Lösung 121.
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 $m \in \operatorname{im} e$ gilt $e(m) = m$, denn es gibt ein $m' \in M$ mit $m = e(m')$, und somit gilt $e(m) = e(e(m')) = e^2(m') = e(m') = m$. Für $m \in \operatorname{im} e \cap \ker e$ folgt, dass $m = e(m) = 0$ gilt; deshalb gilt $\operatorname{im} e \cap \ker e = 0$.

Lösung 122.
Für $\varphi_1, \varphi_2 \in \operatorname{Hom}_R(L, N)$ gilt wegen der Injektivität von f, dass

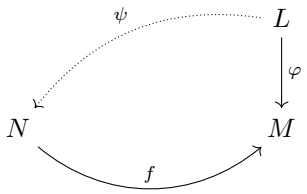
$$f_*(\varphi_1) = f_*(\varphi_2) \iff f \circ \varphi_1 = f \circ \varphi_2 \iff \varphi_1 = \varphi_2.$$

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

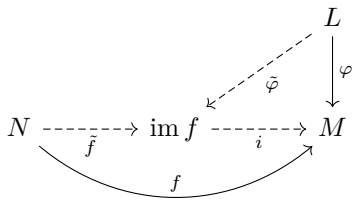
$$(g_* \circ f_*)(\varphi) = g_*(f_*(\varphi)) = \underbrace{g \circ f}_{=0} \circ \varphi = 0,$$

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

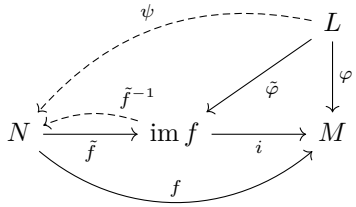
Es sei $\varphi \in \ker g_*$. Um zu zeigen, dass bereits $\varphi \in \operatorname{im} f_*$ gilt, konstruieren wir einen Homomorphismus $\psi\colon L \to N$ mit $\varphi = f_*(\psi) = f \circ \psi$.



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 φ; 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 $f = i \circ \tilde{f}$.



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



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 $\ker g_* \subseteq \operatorname{im} f_*$.

Lösung 123.

(1 $\implies$ 2) Die Sequenz $0 \to \ker g \xrightarrow{i} M \xrightarrow{g} N \to 0$ 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

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

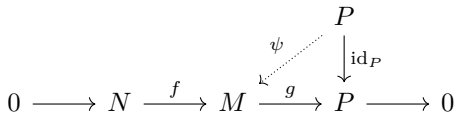
exakt. Inbesondere ist g_* surjektiv, weshalb es für $\varphi \in \operatorname{Hom}_R(P, N)$ ein $\psi \in \operatorname{Hom}_R(P, M)$ mit $\varphi = g_*(\psi) = g \circ \psi$ gibt.

(2 $\implies$ 1) Da $\mathrm{Hom}(P, -)$ linksexakt ist (siehe Übung 122) ist die Sequenz

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

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 $\psi\colon P \to M$ 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:

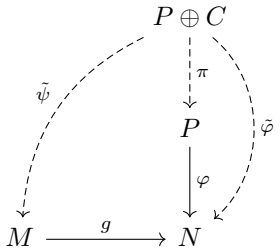


Ein solches ψ existiert nach Annahme.

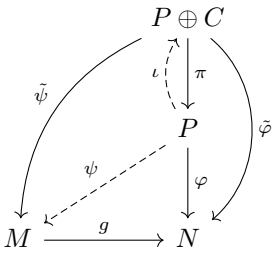
(3 $\implies$ 4) Es gibt einen freien R-Modul F und einen surjektiven Homomorphismus $g\colon F \to P$ (siehe Übung 118). Der Homomorphismus g lässt sich zu einer kurze exakte Sequenz $0 \to \ker g \xrightarrow{i} F \xrightarrow{g} P \to 0$ erweitern, wobei $i\colon \ker g \to F$, $x \mapsto x$ die kanonische 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 $\tilde{\varphi} \coloneqq \varphi \circ \pi\colon P \oplus C \to N$. Da $P \oplus C$ frei ist gibt es, wie bereits gezeigt, einen Homomorphismus $\tilde{\psi}\colon P \oplus C \to M$ mit $g \circ \tilde{\psi} = \tilde{\varphi}$.



Es sei $\iota\colon P \to P \oplus C$, $x \mapsto (x, 0)$ die kanonische Inklusion und $\psi \coloneqq \tilde{\psi} \circ \iota\colon P \to M2$.



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

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

Lösung 124.
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 $f(n) = m \in M'$ gilt, und somit $m = f(n) = f'(n) \in \operatorname{im} f'$. Das zeigt, dass auch $\ker g' \subseteq \operatorname{im} f'$ gilt.

Lösung 125.

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

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

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

Lösung 126.

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

(1 $\implies$ 2) Es sei

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

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

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

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

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

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

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

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

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

von Untermoduln von M, die nicht stabilisiert.

(3 $\implies$ 2) Es sei

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

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

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

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

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

N' widersprechen würde. Also muss bereits $N = N'$ gelten, weshalb N endlich erzeugt ist.

Lösung 127.

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

   $$0 \to f^{-1}(M') \xrightarrow{f'} M' \xrightarrow{g'} g(M') \to 0 \tag{9}$$

   ein, wobei f' und g' die entsprechenden Einschränkungen von f und g bezeichnen (siehe Übung 124). Nach Annahme sind die Untermoduln $f^{-1}(M') \subseteq N$ und $g(M') \subseteq P$ endlich erzeugt. In (9) sind also die beiden äußeren Terme endlich erzeugt, und damit auch der mittlere Term M' (siehe Übung 125).

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 Aussagenteil auch $R^n = R \oplus \cdots \oplus R$ wieder noethersch.

4. Ist M ein R-Modul mit endlichen Erzeugendensystem $\{m_1, \ldots, m_n\} \subseteq M$, so ist der eindeutige Modulhomomorphismus $\varphi\colon R^n \to M$ mit $\varphi(e_i) = m_i$ für alle $i = 1, \ldots, n$ bereits surjektiv. Wir erhalten 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.

Lösung 128.

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

Für $n = 1$ sei $\mathfrak{a} \subseteq R$ ein Untermodul, also ein Ideal. Für $\mathfrak{a} = 0$ ist die Aussage klar, wir beschränken uns also auf den Fall $\mathfrak{a} \neq 0$. Es ist $\mathfrak{a}$ ein Hauptideal, also $\mathfrak{a} = (a)$ für

ein $a \in \mathfrak{a}$, und nach Annahme gilt $a \neq 0$. Die Teilmenge $\{a\} \subseteq \mathfrak{a}$ ist linear unabhängig, denn die Abbildung $R \to \mathfrak{a}$, $r \mapsto ra$ ist injektiv, da R ein Integritätsbereich ist und $a \neq 0$ gilt. Also ist $\{a\}$ eine Basis von $\mathfrak{a}$, und $\mathfrak{a}$ somit frei vom Rang 1.

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

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

$$0 \to i^{-1}(F') \xrightarrow{i'} F' \xrightarrow{p'} p(F') \to 0 \tag{10}$$

ein, wobei i' und p' die entsprechenden Einschränkungen von i und p bezeichnen (siehe Übung 124). 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 (10); inbesondere gilt deshalb $F' \cong i^{-1}(F') \oplus p(F')$. Somit ist F' frei von Rang $\leq n - 1 + 1 = n$.

Lösung 129.

1. Als Hauptidealring ist R insbesondere noethersch. Als endlich erzeugter R-Modul ist M somit ebenfalls noethersch (siehe Übung 127). 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 $i = 1, \ldots, t$ (hier bezeichnet $e_1, \ldots, e_t \in R^t$ die Standardbasis). Dann ist φ surjektiv, und deshalb $F \coloneqq \varphi^{-1}(N)$ ein Untermodul von R^t, für den $\varphi(F) = N$ gilt. Der R-Modul R^t ist frei vom Rang t; da R ein Hauptidealring ist, folgt daraus, dass der Untermodul $F \subseteq R^t$ frei vom Rang $s \leq t$ ist (siehe Übung 128). Ist $b_1, \ldots, b_s \in F$ eine Basis, so bilden $\varphi(b_1), \ldots, \varphi(b_s)$ ein Erzeugendensystem von $\varphi(F) = N$.

Lösung 130.

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 $r_1 m_1 = r_2 m_2 = 0$ gilt. 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 gilt $K = R_S$ für die multiplikative 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 $(m,n) \in T(M \oplus N)$ gibt es $r \in R$ mit $r \neq 0$ und $0 = r(m,n) = (rm, rn)$. Dann gilt $rm = 0$ und $rn = 0$, 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 $r_1 m = 0$, $r_2 n = 0$. Dann gilt $(r_1 r_2)(m,n) = (r_2, r_1 m, r_1 r_2 n) = (0,0)$, 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 $i \in I$ gelten. Da R ein Integritätsbereich ist, folgt zusammen mit $r \neq 0$, dass $r_i = 0$ für alle $i \in I$ gilt. 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 $r_2 m \in T(M)$. 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 $r f(m) = f(rm) = f(0) = 0$ 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

$$T(g) \circ T(f) = T(g \circ f) = T(0) = 0$$

   gilt, und somit $\operatorname{im} T(f) \subseteq \ker T(g)$ gilt. 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 $m = f(n)$ gibt. Da $m \in T(M)$ gilt, gibt es $r \in R$ mit $r \neq 0$ und $0 = rm = r f(n) = f(rn)$. Wegen der Injektivität von f gilt bereits $rn = 0$ und somit $n \in T(N)$. Also gilt $m = f(n) = T(f)(n) \in \operatorname{im} T(f)$ und somit auch $\ker T(g) \subseteq \operatorname{im} T(f)$.

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 $T(\mathbb{Z}) = 0$ gilt folgt daraus, dass $\mathbb{Z}$ als freier $\mathbb{Z}$-Modul torsionfrei ist.)

Lösung 131.
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 $m \in M$ gilt $g(m) \in P$, 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.

Lösung 132.

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 $i \in I$ gilt. Also gilt $\operatorname{im} f \subseteq \ker g$.

   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 $m \in \operatorname{im} f$ gilt. Das zeigt, dass auch $\ker g \subseteq \operatorname{im} f$ gilt.

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.

Lösung 133.

1. Für alle $r \in I$ und $\overline{x} \in R/I$ gilt $rx \in I$ und somit $r\overline{x} = \overline{rx} = 0$. Deshalb gilt $I \subseteq \operatorname{Ann}(R/I)$. Für jedes $r \in \operatorname{Ann}(R/I)$ gilt $\overline{r} = r \cdot \overline{1} = 0$ und somit $r \in I$. Deshalb gilt 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 $x \in F$, so dass $\{x\} \subseteq F$ linear unabhängig ist. Dann gilt $rx \neq 0$ für alle $r \in R$ mit $r \neq 0$, und deshalb $r \notin \operatorname{Ann}(F)$.

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 92). 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 Aussagenteil ist M nicht frei.

Lösung 134.

1. Für jedes Ideal $K \subseteq R$ gilt $\operatorname{Ann}(R/K) = K$ (siehe Übung 133), und somit gilt
$$I = \operatorname{Ann}(R/I) = \operatorname{Ann}(R/J) = J.$$

2. Gilt $R/I \cong R/J$ als Ringe, so gilt nicht notwendigerweise $I = J$. Ist etwa K ein Körper, so ist $K[X]/(X-a) \cong K \cong K[X]/(X-b)$ als Ringe für alle $a, b \in K$, aber $(X-a) \neq (X-b)$ als $K[X]$-Moduln für alle $a \neq b$.

Lösung 135.

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 $m' \in \{rm \mid r \in R\} = \langle m \rangle_R$. Also gilt auch $\operatorname{Ann}(m) \subseteq \operatorname{Ann}(\langle m \rangle_R)$.

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 Gleichheitskette
$$\operatorname{Ann}(\langle m_i \mid i \in I \rangle_R) = \operatorname{Ann}\left(\sum_{i \in I} \langle m_i \rangle_R\right) = \bigcap_{i \in I} \operatorname{Ann}(\langle m_i \rangle_R) = \bigcap_{i \in I} \operatorname{Ann}(m_i)$$
und somit insbesondere $\operatorname{Ann}(M) = \operatorname{Ann}(\langle m_i \mid i \in I \rangle) = \bigcap_{m \in M} \operatorname{Ann}(m)$.

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 $\operatorname{Ann}(M_1 \cap M_2) = \operatorname{Ann}(0) = R \neq 0$.

Lösung 136.
Für die ersten beiden Beispiele 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

$$N_1 = 0 \oplus \bigoplus_{n\geq 1} R = 0 \oplus R \oplus R \oplus \cdots .$$
$$N_2 = 0 \oplus 0 \oplus \bigoplus_{n\geq 2} R = 0 \oplus 0 \oplus R \oplus \cdots$$

   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-Moduls wohldefiniert ist.)

2. Wir betrachten erneut $M_1 = M_2 = \bigoplus_{n\geq 0} R$, dieses Mal mit den jeweiligen Untermoduln

$$N_1 = R \oplus \bigoplus_{n\geq 1} 0 = R \oplus 0 \oplus 0 \oplus \cdots ,$$
$$N_2 = R \oplus R \oplus \bigoplus_{n\geq 2} 0 = R \oplus R \oplus 0 \oplus 0 \oplus \cdots$$

   Dann gelten $M_1 = M_2$ und

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

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

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

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

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

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