Übungen zu Einführung in die Algebra

Jendrik Stelzner

20. November 2016

Inhaltsverzeichnis

1 Gruppentheorie

Übung 1. *Ein Kriterium für maximale Untergruppen*

Es sei G ein Gruppe und $H \subseteq G$ eine Untergruppe, so dass $[G : H]$ endlich und prim ist. Zeigen Sie, dass H eine maximale echte Untergruppe von G ist. Entscheiden Sie, ob H notwendigerweise normal in G ist.

Lösung 1.

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

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

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

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

Übung 2. *Multiple Choice I*

Entscheiden Sie, ob die folgenden Aussagen allgemein gültig sind, und geben sie gegebenenfalls ein Gegenbeispiel an.

1. Ist G eine Gruppe und $N \subseteq G$ eine normale Untergruppe, so gilt $G \cong (G/N) \times N$.
2. Ist G eine endliche Gruppe, so dass G/N für normale Untergruppe $N \subseteq G$ mit $N \neq 1$ abelsch ist, so ist auch G abelsch.
3. Zwei Gruppen G_1 und G_2 sind genau dann isomorph, wenn $G_1 \times H \cong G_2 \times H$ für jede Gruppe H.
4. Sind G_1 und G_2 zwei Gruppen, so ist jede Untergruppe von $G_1 \times G_2$ von der Form $H_1 \times H_2$ für Untergruppen $H_1 \subseteq G_1$ und $H_2 \subseteq G_2$.
5. Sind G_1 und G_2 zwei Gruppen, so dass es Gruppenepimorphismen $\phi\colon G_1 \to G_2$ und $\psi\colon G_2 \to G_1$ gibt, so gilt $G_1 \cong G_2$.

Lösung 2.

1. Die Aussage ist falsch: Es sei $G = \mathbb{Z}$ und $N = 2\mathbb{Z}$. Dann ist

   $$(G/N) \times N \cong (\mathbb{Z}/2\mathbb{Z}) \times (2\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}.$$

   Es ist allerdings $(\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z} \ncong \mathbb{Z}$, da $(\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$ ein Element der Ordnung 2 enthält (nämlich $(1, 0)$), $\mathbb{Z}$ aber nicht.

2. Die Aussage ist falsch: Die einzige nicht-trivialen normalen Untergruppe von S_3 sind $N = \langle(1\,2\,3)\rangle = \{\mathrm{id}, (1\,2\,3), (1\,3\,2)\}$ und S_3 selbst. Der Quotient S_3/N hat Ordnung 2, weshalb $S_3/N \cong \mathbb{Z}/2\mathbb{Z}$ abelsch ist, und $S_3/S_3 = 1$ ist ohnehin abelsch. Die Gruppe S_3 selbst ist allerdings nicht abelsch.

   Alternativ ist A_n für $n \geq 5$ einfach, weshalb A_n der einzige nicht-triviale Normalteiler von A_n ist, aber A_4 ist für $n \geq 4$ nicht abelsch.

3. Die Aussage ist wahr: Gilt $G_1 \cong G_2$, so gibt es einen Isomorphismus $\phi\colon G_1 \to G_2$. Für jede Gruppe H ist dann $\phi \times \mathrm{id}_H\colon G_1 \times H \to G_2 \times H$ ein Isomorphismus, und somit $G_1 \times H \cong G_2 \times H$. Gilt andererseits $G_1 \times H \cong G_2 \times H$ für jede Gruppe H, so gilt inbesondere $G_1 \cong G_1 \times 1 \cong G_2 \times 1 \cong G_2$.

4. Die Aussage ist falsch: Ist $G \neq 1$ eine Gruppe und $G_1 = G_2 = G$, so ist die Diagonale $\Delta = \{(g,g) \mid g \in G\}$ eine Untergruppe von $G_1 \times G_2 = G \times G$, die sich nicht als ein solches Produkt schreiben lässt.

5. Die Aussage ist falsch: Für die Gruppen

   $$G_1 = \bigoplus_{n \in \mathbb{N}} \mathbb{Z} = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots$$

   und

   $$G_2 = \mathbb{Z}/2\mathbb{Z} \oplus \bigoplus_{n \in \mathbb{N}} \mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots$$

   gibt es Gruppenepimorphismen

   $$\phi\colon G_1 \to G_2, \quad (n_1, n_2, n_3, \dots) \mapsto (\overline{n_1}, n_2, n_3, \dots)$$

   und

   $$\psi\colon G_2 \to G_1, \quad (\overline{n_1}, n_2, n_3, \dots) \mapsto (n_2, n_3, \dots).$$

   Es gilt aber $G_1 \ncong G_2$, denn G_2 enthält ein Element der Ordnung 2, G_1 jedoch nicht.

Übung 3.
Es seien G_1 und G_2 zwei Gruppen, $N_1 \subseteq G_1$ und $N_2 \subseteq G_2$ zwei normale Untergruppen. Geben Sie jeweils Beispiele für die folgenden Situationen:

1. Es gilt $G_1 \cong G_2$ und $N_1 \cong N_2$, aber $G_1/N_1 \ncong G_2/N_2$.
2. Es gilt $G_1 \cong G_2$ und $G_1/N_1 \cong G_2/N_2$, aber $N_1 \ncong N_2$.
3. Es gilt $G_1/N_1 \cong G_2/N_2$ und $N_1 \cong N_2$, aber $G_1 \ncong G_2$.

Lösung 3.

1. Es seien $G_1 = G_2 = \bigoplus_{n\geq 0} \mathbb{Z}$, sowie $N_1 = \bigoplus_{n\geq 1} \mathbb{Z}$ und $N_2 = \bigoplus_{n\geq 2} \mathbb{Z}$. Dann gilt $G_1 = G_2 \cong N_1 \cong N_2$ aber
$$G_1/N_1 \cong \mathbb{Z} \ncong \mathbb{Z} \oplus \mathbb{Z} = G_2/N_2.$$

2. Es seien $G_1 = G_2 = \bigoplus_{n\geq 0} \mathbb{Z}$ und
$$N_1 \coloneqq \mathbb{Z} \oplus 0 \oplus 0 \oplus 0 \oplus \cdots$$
und
$$N_2 \coloneqq \mathbb{Z} \oplus \mathbb{Z} \oplus 0 \oplus 0 \oplus \cdots$$
Dann gilt
$$G_1/N_1 \cong \bigoplus_{n\geq 1} \mathbb{Z} \cong \bigoplus_{n\geq 2} \mathbb{Z} = G_2/N_2.$$
Es gilt aber $N_1 \ncong N_2$, denn $N_1 \cong \mathbb{Z}$ ist zyklisch, $\mathbb{Z} \oplus \mathbb{Z}$ aber nicht.

3. Es seien $G_1 = \mathbb{Z}/4\mathbb{Z}$ und $G_2 = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, sowie $N_1 = 2\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{2}\}$ und $N_2 = \mathbb{Z}/2\mathbb{Z} \oplus 0$. Wegen der Kommutativität von G_1 und G_2 handelt es sich jeweils um eine normale Untergruppe. Da N_1 und N_2 beide zweielementig sind, gilt
$$N_1 \cong \mathbb{Z}/2\mathbb{Z} \cong N_2$$
(denn $\mathbb{Z}/2\mathbb{Z}$ ist die bis auf Isomorphie eindeutige zweielementige Gruppe). Nach dem zweiten (oder dritten) Isomorphiesatz gilt
$$G_1/N_1 = (\mathbb{Z}/4\mathbb{Z})/(2\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z},$$
und für den anderen Quotienten gilt
$$\begin{aligned} G_2/N_2 &= (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z})/(\mathbb{Z}/2\mathbb{Z} \oplus 0) \\ &\cong ((\mathbb{Z}/2\mathbb{Z})/(\mathbb{Z}/2\mathbb{Z})) \oplus ((\mathbb{Z}/2\mathbb{Z})/0) \cong 0 \oplus \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}. \end{aligned}$$
Also gilt auch $G_1/N_1 \cong G_2/N_2$. Es gilt aber $G_1 \ncong G_2$, da G_1 ein Element der Ordnung 4 enthält, G_2 jedoch nicht.

Übung 4. *Gruppen mit trivialer Automorphismengruppe*
Es sei G eine Gruppe mit $\mathrm{Aut}(G) = 1$.

1. Zeigen Sie, dass G abelsch ist.
2. Zeigen Sie, dass $g = -g$ für alle $g \in G$.
3. Folgern Sie, dass es eine eindeutige $\mathbb{F}_2$-Vektorraumstruktur auf G gibt.
4. Folgern Sie, dass $G = 0$ oder $G \cong \mathbb{Z}/2\mathbb{Z}$.

Lösung 4.

1. Für $g \in G$ sei $c_g\colon G \to G$ die Konjugation mit g. Dies ist ein Automorphismus von G, weshalb $c_g = \mathrm{id}_G$. Somit ist $g \in \mathrm{Z}(G)$.

2. Wegen der Kommutativität von G ist die Abbildung $n\colon G \to G$, $g \mapsto -g$ ein Automorphismus von G. Somit ist $n = \mathrm{id}_G$, also $-g = g$ für alle $g \in G$.

3. Nach dem vorherigen Aufgabenteil ist $2g = 0$ für alle $g \in G$. Deshalb gibt es eine eindeutige $\mathbb{F}_2$-Vektorraumstruktur auf G via

$$\overline{n} \cdot g = n \cdot g \quad \text{für alle } n \in \mathbb{Z}, g \in G,$$

wie sich durch direktes Nachrechnen ergibt.

4. Es sei $(b_i)_{i \in I}$ eine Basis von G als $\mathbb{F}_2$-Vektorraum. Ist $G \neq 0$ und $G \ncong \mathbb{Z}/2$, so ist $\dim_{\mathbb{F}_2} G \geq 2$. Es gibt daher $i_1, i_2 \in I$ with $i_1 \neq i_2$. Die Permutation

$$\sigma\colon \{b_i\}_{i \in I} \to \{b_i\}_{i \in I}, \quad b_j \mapsto \begin{cases} b_{i_2} & \text{falls } j = i_1, \\ b_{i_1} & \text{falls } j = i_2, \\ b_j & \text{sonst,} \end{cases}$$

induziert einen nicht-trivialen $\mathbb{F}_2$-Vektorraumautomorphismus $\alpha\colon G \to G$ mit

$$\alpha\left(\sum_{i \in I} \lambda_i b_i\right) = \sum_{i \in I} \lambda_i b_{\sigma(i)}.$$

Dann ist α aber insbesondere ein nicht-trivialer Gruppenautomorphismus, im Widerspruch zu $\mathrm{Aut}(G) = 1$.

2 Ringtheorie

Übung 5. *Initialobjekte in der Kategorie der Ringe*

1. Zeigen Sie, dass es für jeden Ring R einen eindeutigen Ringhomomorphismus $\mathbb{Z} \to R$ gibt. (Dies bedeutet, dass der Ring $\mathbb{Z}$ ein Initialobjekt in der Kategorie der Ringe ist.)

2. Es sei Z ein Ring, so dass es für jeden Ring R einen eindeutigen Ringhomomorphismus $Z \to R$ gibt. Zeigen Sie, dass $Z \cong \mathbb{Z}$.

Lösung 5.

1. Ist $\phi\colon \mathbb{Z} \to R$ ein Ringhomomorphismus, so ist $\phi(1_\mathbb{Z}) = 1_R$. Für alle $n \in \mathbb{Z}$ ist damit
$$\phi(n) = \phi(n \cdot 1_\mathbb{Z}) = n \cdot \phi(1_\mathbb{Z}) = n \cdot 1_R.$$
Also ist ϕ eindeutig. Durch direktes Nachrechnen ergibt sich auch, dass $\psi\colon \mathbb{Z} \to R$ mit
$$\psi(n) \coloneqq n \cdot 1_R \quad \text{für alle } n \in \mathbb{Z}$$
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 $\mathrm{id}_\mathbb{Z}\colon \mathbb{Z} \to \mathbb{Z}$ ebenfalls ein Ringhomomorphismus ist. Da es genau einen Ringhomomorphismus $\mathbb{Z} \to \mathbb{Z}$ gibt, muss sowohl $\psi \circ \phi$ als auch $\mathrm{id}_\mathbb{Z}$ dieser eindeutige Ringhomomorphismus $\mathbb{Z} \to \mathbb{Z}$ sein. Folglich ist $\psi \circ \phi = \mathrm{id}_\mathbb{Z}$. Analog ergibt sich, dass $\phi \circ \psi = \mathrm{id}_Z$.

Übung 6.

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

Lösung 6.

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

Übung 7.
Es sei R ein kommutativer Ring.

1. Zeigen Sie, dass ein Ideal $\mathfrak{p} \subseteq R$ genau dann prim ist, wenn $R/\mathfrak{p}$ ein Integritätsbereich ist.
2. Zeigen Sie, dass ein Ideal $\mathfrak{m} \subseteq R$ genau dann maximal ist, wenn $R/\mathfrak{m}$ ein Körper ist.

Lösung 7.
Dies ist eine Standardaussage, deren Beweis sich in jedem Algebra-Buch findet.

Übung 8.
Es sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal.

1. Definieren Sie das Radikal $\sqrt{I}$ und zeigen Sie, dass $\sqrt{I}$ ebenfalls ein Ideal ist.
2. Zeigen Sie, dass $\sqrt{\sqrt{I}} = \sqrt{I}$.
3. Zeigen Sie, dass $\sqrt{I}$ genau dann ein echtes Ideal ist, wenn I ein echtes Ideal ist.

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

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

Übung 9.
Es sei R ein kommutativer Ring und $\mathfrak{p} \subseteq R$ ein Ideal. Zeigen Sie, dass $\mathfrak{p}$ genau dann ein Primideal ist, wenn es einen Körper K und einen Ringhomomorphismus $\phi\colon R \to K$ mit $\ker \phi = \mathfrak{p}$ gibt.

Lösung 9.
Ist $\mathfrak{p}$ ein Primideal, so ist der Quotient $R/\mathfrak{p}$ ein Integritätsbereich. Da die kanonische Inklusion $R/\mathfrak{p} \to Q(R/\mathfrak{p})$ ein injektiver Ringhomomorphismus ist, folgt für die Komposition

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

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

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

Übung 10.
Es sei K ein Körper.

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

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

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

Übung 11. *Funktorialität der Einheitengruppe*
Ist R ein Ring, so ist

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

die *Einheitengruppe* von R. Zeigen Sie:

1. Ist R ein Ring, so bildet $R^\times$ bezüglich der Multiplikation aus R eine Gruppe.

2. Sind R und S zwei 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 R gilt $\mathrm{id}_R^\times = \mathrm{id}_{R^\times}$, und für alle Ringhomomorphismen $\phi \colon R_1 \to R_2$ und $\psi \colon R_2 \to R_3$ gilt $(\psi\phi)^\times = \psi^\times \phi^\times$.

(*Hinweis*: Zum Verständnis genügt es kommutative Ringe zu betrachten. Die Aussage ist aber auch für nicht-kommutative Ringe von Bedeutung.)

Übung 12. *Urbilder von Idealen*
Es seien R und S zwei kommutative Ringe und $\phi \colon R \to S$ ein Ringhomomorphismus.

1. Zeigen Sie, dass für jedes Ideal $\mathfrak{a} \subseteq S$ das Urbild $\phi^{-1}(\mathfrak{a})$ ein Ideal in R ist.

2. Entscheiden Sie, ob $\phi^{-1}(\mathfrak{p})$ ein Primideal ist, wenn $\mathfrak{p} \subseteq S$ ein Primideal ist.

3. Entscheiden Sie, ob $\phi^{-1}(\mathfrak{m})$ ein maximales Ideal ist, wenn $\mathfrak{m} \subseteq S$ ein maximales Ideal ist.

Lösung 12.

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

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

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

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

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

Übung 13.

Es sei R ein kommutativer Ring. Es seien $\mathfrak{a}, \mathfrak{b} \subseteq R$ zwei Ideale mit $\mathfrak{a} = (x_i \mid i \in I)$ und $\mathfrak{b} = (y_j \mid j \in J)$. Zeigen Sie, dass

$$\mathfrak{a}\mathfrak{b} = (x_i y_j \mid i \in I, j \in J).$$

Lösung 13.

Für alle $i \in I$ und $j \in J$ folgt aus $x_i \in \mathfrak{a}$ und $y_j \in \mathfrak{b}$, dass $x_i y_j \in \mathfrak{a}\mathfrak{b}$. Daraus folgt, dass $(x_i y_j \mid i \in I, j \in J) \subseteq \mathfrak{a}\mathfrak{b}$. Sind andererseits $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$, so ist $a = \sum_{i \in I} r_i x_i$ und $b = \sum_{j \in J} s_j y_j$ mit $r_i, s_j \in R$, wobei $r_i = 0$ für fast alle $i \in I$ und $s_j = 0$ für fast alle $j \in J$. Deshalb ist

$$ab = \sum_{\substack{i \in I \\ j \in J}} r_i s_j x_i y_j \in (x_i y_j \mid i \in I, j \in J).$$

Da jedes Element aus $\mathfrak{a}\mathfrak{b}$ von der Form $\sum_{k=1}^{n} a_k b_k$ mit $a_k \in \mathfrak{a}$ und $b_k \in \mathfrak{b}$ ist, folgt daraus, dass $\mathfrak{a}\mathfrak{b} \subseteq (x_i y_j \mid i \in I, j \in J)$.

Übung 14. *Zur Definition von Unterringen*

Geben Sie ein Beispiel für einen kommutativen Ring R und eine Teilmenge $S \subseteq R$ mit den folgenden Eigenschaften:

- S ist abgeschlossen unter der Addition und Multiplikation von R, d.h. für alle $s_1, s_2 \in S$ ist auch $s_1 + s_2 \in S$ und $s_1 s_2 \in S$.
- Zusammen mit der Einschränkung der Addition und Multiplikation aus R ist S ebenfalls ein (notwendigerweise kommutativer) Ring.
- S ist kein Unterring von R.

Lösung 14.

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

Übung 15.

Es sei R ein kommutativer Ring.

1. Definieren Sie, wann zwei Elemente von R assoziiert sind.
2. Es sei nun R ein Integritätsbereich. Zeigen Sie, dass zwei Elemente $a, b \in R$ genau dann assoziiert sind, wenn $(a) = (b)$.

Übung 16.
Es sei R ein kommutativer Ring und $S \subseteq R$ eine multiplikative Teilmenge.

1. Zeigen Sie, dass R_S noethersch ist, wenn R noethersch ist.
2. Zeigen oder widerlegen Sie, dass R_S ein Hauptidealring ist, wenn R ein Hauptidealring ist.

Übung 17.
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 18.
Für jedes $d \in \mathbb{N}$ sei

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

Es darf im Folgenden ohne Beweis genutzt werden, dass $\mathbb{Z}[\sqrt{-d}]$ ein Unterring von $\mathbb{C}$ ist.

1. Zeigen Sie, dass $\mathbb{Z}[\sqrt{-1}]$ ein euklidischer Ring ist.
2. Zeigen Sie, dass $\mathbb{Z}[\sqrt{-2}]$ ein euklidischer Ring ist.
3. Zeigen Sie, dass $\mathbb{Z}[\sqrt{-5}]$ kein euklidischer Ring ist.

Übung 19.
Es sei R ein euklidischer Ring. Zeigen Sie, dass R ein Hauptidealring ist.

Übung 20.
Es sei R ein kommutativer Ring, so dass $R[X]$ ein Hauptidealring ist. Zeigen Sie, dass R bereits ein Körper ist.

Übung 21.
Es sei K ein Körper. Zeigen Sie, dass es in $K[X]$ unendlich viele irreduzible, normierte Polynome gibt.

Übung 22.
Es seien R und R' zwei kommutative Ringe, $S \subseteq R$ eine multiplikative Teilmenge und $f\colon R \to R'$ ein Ringhomomorphismus.

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

Übung 23.
Es sei R ein kommutativer Ring.

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

2. Zeigen Sie, dass $\mathfrak{p}[X]$ ein Primideal in $R[X]$, wenn $\mathfrak{p} \subseteq R$ ein Primideal ist.

3. Zeigen oder widerlegen Sie, dass $\mathfrak{m}[X]$ notwendigerweise ein maximales Ideal in $R[X]$ ist, wenn $\mathfrak{m} \subseteq R$ ein maximales Ideal ist.

Lösung 23.

1. Die kanonische Projektion $\pi\colon R \to R/\mathfrak{a}$, $x \mapsto \overline{x}$ induziert nach der universellen Eigenschaft des Polynomrings $R[X]$ einen Ringhomomorphismus $\varphi\colon R[X] \to (R/\mathfrak{a})[X]$ mit $\varphi|_R = \pi$ und $\varphi(X) = \pi(X)$, und dieser ist gegeben durch
$$\varphi\left(\sum_i f_i X^i\right) = \sum_i \pi(f_i) X^i = \sum_i \overline{f_i} X^i.$$
Für $f = \sum_i f_i X^i \in R[X]$ ist genau dann $f \in \ker \varphi$, wenn $\overline{f_i} = 0$ für alle i, also genau dann, wenn $f_i \in \ker \pi = \mathfrak{a}$ für alle i. Somit ist $\ker \varphi = \mathfrak{a}[X]$ ein Ideal in $R[X]$.

2. Es seien π und φ wie zuvor. Wegen der Surjektivität von π ist auch φ surjektiv. Somit induziert φ einen Ringisomorphismus
$$\psi\colon R[X]/\mathfrak{p}[X] \to (R/\mathfrak{p})[X], \quad \overline{\sum_i f_i X^i} \mapsto \sum_i \overline{f_i} X^i.$$
Der Quotient $R/\mathfrak{p}$ ist ein Integritätsbereich, da $\mathfrak{p}$ ein Primideal in R ist. Somit ist auch $(R/\mathfrak{p})[X]$ ein Integritätsbereich. Da der Quotient $R[X]/\mathfrak{a}[X]$ ein Integritätsbereich ist, folgt, dass $\mathfrak{p}[X]$ ein Primideal in $R[X]$ ist.

3. Ist K ein Körper, so ist $0 \subseteq K$ ein maximales Ideal, und es gilt $\mathfrak{m}[X] = 0$. Der Quotient $K[X]/\mathfrak{m}[X] \cong (K/0)[X] \cong K[X]$ ist kein Körper, da $0 \neq X \in K[X]$ keine Einheit ist. Also ist $\mathfrak{m}[X]$ nicht maximal in $K[X]$.

   Tatsächlich kann $\mathfrak{m}[X]$ nicht maximal in $R[X]$ sein, da $R[X]/\mathfrak{m}[X] \cong (R/\mathfrak{m})[X]$, aber es keinen Ring R' gibt, so dass $R'[X]$ ein Körper ist (siehe Übung 24).

Übung 24.
Zeigen Sie, dass es keinen Ring R gibt, so dass $R[X]$ ein Körper ist.

Lösung 24.
Gebe es einen solchen Ring R, so wäre R kommutativ, da $R \subseteq R[X]$ ein Unterring ist. Es wäre auch $R \neq 0$ da $0[X] = 0$ kein Körper ist. Dann wäre aber $0 \neq X \in R[X]$ keine Einheit und $R[X]$ somit kein Körper.

Übung 25.
Zeigen Sie, dass $\mathbb{Z}[i] \cong \mathbb{Z}[X]/(X^2+1)$.

Übung 26.
Es sei R ein kommutativer Ring und $f \in R$. Zeigen Sie, dass $R_f \cong R[X]/(fX-1)$.

Lösung 26.
Das Element $\overline{f} \in R[X]/(fX-1)$ ist eine Einheit mit $\overline{f}^{-1} = \overline{X}$ da

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

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

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

Andererseits induziert der kanonische Ringhomomorphismus $i\colon R \to R_f$, $r \mapsto r/1$ nach der universellen Eigenschaft des Polynomrings $R[X]$ einen eindeutigen Ringhomomorphismus $\tilde{\psi}\colon R[X] \to R_f$ mit $\tilde{\psi}|_R = i$ und $\tilde{\psi}(X) = 1/f$, und dieser ist gegeben durch

$$\tilde{\psi}\left(\sum_i r_i X^i\right) = \sum_i \frac{r_i}{f^i}.$$

Dann gilt insbesondere

$$\tilde{\psi}(fX-1) = \tilde{\psi}(f)\tilde{\psi}(X) - \tilde{\psi}(1) = \frac{f}{1}\frac{1}{f} - \frac{1}{1} = 0.$$

Also faktorisiert $\tilde{\psi}$ über einen eindeutigen Ringhomomorphismus $\psi\colon R[X]/(fX-1) \to R_f$ mit $\psi(\overline{p}) = \tilde{\psi}(p)$ für alle $p \in R[X]$, d.h. es ist

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

Die beiden Ringhomomorphismen φ und ψ sind invers zueinander: Für alle $r/f^k \in R_f$ gilt

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

und für alle $\sum_i r_i X^i \in R[X]$ gilt

$$\varphi\left(\psi\left(\overline{\sum_i r_i X^i}\right)\right) = \varphi\left(\sum_i \frac{r_i}{f^i}\right) = \sum_i \varphi\left(\frac{r_i}{f^i}\right) = \overline{\sum_i r_i X^i}.$$

Also ist φ ein Isomorphismus mit $\varphi^{-1} = \psi$.

Übung 27.
Bestimmen Sie die Einheitengruppe $\mathbb{Z}[i]^\times$.

Lösung 27.
Ein Element $z \in \mathbb{Z}[i]$ ist genau dann eine Einheit in $\mathbb{Z}[i]$, wenn $z \neq 0$ und $z^{-1} \in \mathbb{Z}[i]$ (hier bezeichnet $z^{-1} = 1/z$ das Inverse von z in $\mathbb{C}$). Für die Elemente $1, -1, i, -i \in \mathbb{Z}[i]$ ist dies erfüllt. Ist $z \in \mathbb{Z}[i]$ mit $z \neq 0$ und $z^{-1} \in \mathbb{Z}[i]$, so ist

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

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

3 Modultheorie

Übung 28.
Zeigen Sie, dass es auf jeder abelschen Gruppe genau eine $\mathbb{Z}$-Modulstruktur gibt.

Übung 29.
Es sei R ein kommutativer Ring und M ein R-Modul. Es sei $I \subseteq R$ ein Ideal.

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

2. Es sei $S \subseteq R$ eine multiplikative Teilmenge. Zeigen Sie, dass sich die R-Modulstruktur auf M genau dann zu einer R_S-Modulstruktur fortsetzen lässt, wenn für jedes $s \in S$ die Abbildung $\lambda_s \colon M \to M$, $m \mapsto sm$ bijektiv ist.

Übung 30.
Es sei M ein endlich erzeugter R-Modul. Zeigen Sie, dass jedes Erzeugendensystem $S \subseteq M$ ein endliches Erzeugendensystem enthält.

Lösung 30.
Es sei $\{m_1, \ldots, m_s\} \subseteq M$ ein endliches Erzeugendensystem. Da S ein Erzeugendensystem ist, lässt sich jedes m_i als $m_i = r_{i,1}s_{i,1} + \cdots + r_{i,t_i}s_{i,t_i}$ mit $t_i \geq 0$, $s_{i,1}, \ldots, s_{i,t_i} \in S$ und $r_{i,1}, \ldots, r_{i,t_i} \in R$ schreiben. Für $S' \coloneqq \{s_{i,j} \mid i = 1, \ldots, s, j = 1, \ldots, t_i\}$ gilt dann $m_i \in \langle S \rangle$ für alle $i = 1, \ldots, s$ und deshalb

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

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

Übung 31.
Es sei $0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0$ eine kurze exakte Folge 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.

4 Körpertheorie

Übung 32.
Zeigen Sie, dass für einen kommutativen Ring K die folgenden Bedingungen äquivalent sind:

1. K ist ein Körper.
2. K hat genau zwei Ideale.
3. Das Nullideal in K ist maximal.

Lösung 32.
($1 \implies 2$) Da K ein Körper ist gilt $0 \neq K$, also hat K mindestens zwei Ideale. Ist $I \subseteq K$ ein Ideal mit $I \neq 0$, so gibt es ein $x \in I$ mit $x \neq 0$. Dann ist x eine Einheit in K, somit $K = (x) \subseteq I$ und deshalb $I = K$. Also sind 0 und K die einzigen Ideale in K.

($2 \implies 3$) Es muss $0 \neq K$, denn sonst wäre 0 das einzige Ideal in K. Also sind 0 und K die einzigen beiden Ideale in K. Ist $I \subseteq K$ ein Ideal mit $0 \subsetneq I$, so muss bereits $I = K$. Also ist 0 ein maximales Ideal.

($3 \implies 1$) Da $0 \subseteq K$ maximal ist, ergibt sich, dass $K \cong K/0$ ein Körper ist.

Übung 33.
Es sei K ein algebraisch abgeschlossener Körper. Zeigen Sie, dass K unendlich ist.

Lösung 33.
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.