Algebra I (LAG) **Klausur vom 10.04.2025**

A1	A2	A3	A4	A5	A6	A7	Σ
10	10	10	10	10	10	10	70

Hinweise

- Diese Klausur besteht aus 7 Aufgaben in denen jeweils 10 Punkte erreicht werden können. Die mögliche Gesamtpunktzahl beträgt also 70 Punkte.
- Bearbeiten Sie die Aufgaben bitte direkt unter der Aufgabenstellung. Sollte der Platz nicht ausreichen, fahren Sie auf der entsprechenden Rückseite (oder Rückseite des vorherigen Blatts) fort und kennzeichnen Sie dies entsprechend.
- Begründen Sie Ihre Aussagen.
- Die Bearbeitungszeit beträgt 180 Minuten.
- Neben Schreibzeug, Ausweis/Studierendenausweis und Verpflegung dürfen keine weiteren Hilfsmittel mit an den zugewiesenen Arbeitsplatz genommen werden.
- Sie dürfen innerhalb einer Aufgabe einen vorangegangenen Aufgabenteil auch dann verwenden, wenn Sie diesen Teil nicht bearbeitet haben.

Viel Erfolg!

Algebra I (LAG) **Klausur vom 10.04.2025**

Aufgabe 1. Entscheiden Sie jeweils, ob die folgenden Aussagen wahr oder falsch sind und setzen Sie bei jeder Aussage genau ein Kreuz. Richtig gesetzte Kreuze geben 1 Punkt und falsch gesetzte Kreuze geben keinen Punkt. Wenn Sie ein gesetztes Kreuz korrigieren wollen, füllen Sie die Box mit dem falsch gesetzten Kreuz aus und markieren Sie die andere Box mit einem Kreuz.

(1) Entscheiden Sie bei den folgenden Aussagen, ob diese für **jeden** Integritätsbereich R richtig sind.

Ist $p \in R$ irreduzibel, so ist p kein Primelement.	☐ wahr	☐ falsch
Ist $a \in R$ mit $a^2 = 0$, so ist $1 - a$ eine Einheit.	☐ wahr	☐ falsch
Sind $a, b, c \in R$ mit $ac = bc$, so gilt $a = b$.	☐ wahr	☐ falsch
Es ist R ist ein faktorieller Ring.	☐ wahr	☐ falsch
Ist R endlich, so existiert eine Primzahl $p \in \mathbb{P}$ und ein Isomorphismus von Ringen $R \cong \mathbb{Z}/(p)$.	☐ wahr	☐ falsch

(2) Entscheiden Sie bei den folgenden Aussagen, ob diese für **jede** endliche Gruppe G richtig sind.

Für alle Untergruppen $U, V \subseteq G$ ist UV eine Untergruppe.	☐ wahr	☐ falsch
Gilt $\lvert G\rvert = 12$, so besitzt G eine Untergruppe der Ordnung 6.	☐ wahr	☐ falsch
Gilt $\lvert G\rvert = 24$, so besitzt G eine Untergruppe der Ordnung 8.	☐ wahr	☐ falsch
Für jede Gruppe H und jeden injektiven Homomorphismus von Gruppen $\varphi\colon G \longrightarrow H$ ist $\varphi(G)$ ein Normalteiler von H.	☐ wahr	☐ falsch
Besitzt G eine Untergruppe der Ordnung 5, so gilt $\lvert G\rvert \neq 12$.	☐ wahr	☐ falsch

Aufgabe 2. (4+4+2 Punkte) Es bezeichne $\mathcal{S}_9$ die symmetrische Gruppe auf der Menge $\{1,\dots,9\}$. Es seien die Elemente $\sigma_1 := (1,9)\circ(3,4)\circ(2,9)$ und $\sigma_2 := (2,7)\circ(4,3,5)\circ(4,3,5)\circ(8,6)\circ(2,7)$ in $\mathcal{S}_9$ gegeben.

(1) Existiert ein Element $\tau \in \mathcal{S}_9$ mit $\tau\circ\sigma_1\circ\tau^{-1} = \sigma_2$? Wenn ein solches Element existiert, geben Sie ein solches Element an.

(2) Es sei $\sigma \in \mathcal{S}_9$. Geben Sie die Definition des Trägers $\operatorname{supp}(\sigma)$ von σ. Weiter seien $\sigma_3 := (1,2)\circ(7,2)$ und $\sigma_4 \in \mathcal{S}_9$ mit $\operatorname{supp}(\sigma_3)\cap\operatorname{supp}(\sigma_4) = \varnothing$. Berechnen Sie $\sigma_4\circ\sigma_3^{101}\circ\sigma_4^{-1}$.

(3) Es sei N ein Normalteiler von $\mathcal{S}_9$ mit $(1,2)\in N$. Zeigen Sie, dass $N = \mathcal{S}_9$ gilt. **Hinweis:** Für $n\geq 2$ gilt $\mathcal{S}_n = \langle\{(1,i)\mid i\in\{2,\dots,n\}\}\rangle$.

Lösung:

(1) Es gilt $\sigma_1 = (1,9,2)\circ(3,4)$ und $\sigma_2 = (4,5,3)\circ(8,6)$. Es sei

$$\tau := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 3 & 8 & 6 & 1 & 2 & 7 & 9 & 5 \end{pmatrix} \in \mathcal{S}_9.$$

Dann gilt

$$\begin{aligned} \tau\circ\sigma_1\circ\tau^{-1} &= (\tau\circ(1,9,2)\circ\tau^{-1})\circ(\tau\circ(3,4)\circ\tau^{-1}) \\ &= (\tau(1),\tau(9),\tau(2))\circ(\tau(3),\tau(4)) \\ &= (4,5,3)\circ(8,6) = \sigma_2. \end{aligned}$$

(2) Es ist $\operatorname{supp}(\sigma) = \{i\in\{1,\dots,9\}\mid\sigma(i)\neq i\}$. Mit $\operatorname{supp}(\sigma_3)\cap\operatorname{supp}(\sigma_4) = \varnothing$ gilt nach Vorlesung (Bemerkung 1.7.4) $\sigma_3\circ\sigma_4 = \sigma_4\circ\sigma_3$ und damit

$$\sigma_4\circ\sigma_3^{101}\circ\sigma_4^{-1} = \sigma_3^{101}\circ\sigma_4\circ\sigma_4^{-1} = \sigma_3^{101} = ((\sigma_3)^3)^{33}\circ\sigma_3^2.$$

Es ist $\sigma_3 = (1,2,7)$ ein 3-Zykel und damit gilt $\sigma_3^3 = \mathrm{id}$ und $\sigma_3^2 = (1,7,2)$. Wir erhalten

$$\sigma_4\circ\sigma_3^{101}\circ\sigma_4^{-1} = ((\sigma_3)^3)^{33}\circ\sigma_3^2 = \mathrm{id}^{33}\circ\sigma_3^2 = (1,7,2).$$

Alternativ berechnet man:

$$\sigma_4\circ\sigma_3^{101}\circ\sigma_4^{-1} = (\sigma_4\circ\sigma_3\circ\sigma_4^{-1})^{101} = (\sigma_4(1),\sigma_4(2),\sigma_4(7))^{101} = (1,2,7)^{101},$$

da $1,4,7\in\operatorname{supp}(\sigma_3)$ und damit $1,4,7\in\operatorname{supp}(\sigma_4)$. Nun rechnet man weiter wie oben.

(3) Es sei $i\in\{3,\dots,9\}$. Dann gilt $(2,i)\circ(1,2)\circ(2,i)^{-1} = ((2,i)(1),(2,i)(2)) = (1,i)$. Da N ein Normalteiler ist, gilt damit $(1,i)\in N$. Es folgt $\{(1,2),(1,3),\dots,(1,9)\}\subseteq N$. Nach dem Hinweis gilt damit $\mathcal{S}_9 = \langle\{(1,2),(1,3),\dots,(1,9)\}\rangle\subseteq\langle N\rangle = N$, da N eine Untergruppe von $\mathcal{S}_9$ ist. Weiter gilt $N\subseteq\mathcal{S}_9$ und damit $N = \mathcal{S}_9$.

Aufgabe 3. (4+1+3+2 Punkte) Es sei G eine endliche Gruppe und $U \subseteq G$ eine Untergruppe.

(1) Zeigen Sie, dass $N_G(U) := \{g \in G \mid gUg^{-1} = U\}$ eine Untergruppe von G ist und $U \subseteq N_G(U)$ gilt.
(2) Zeigen Sie, dass U ein Normalteiler von $N_G(U)$ ist und dass jede Untergruppe $H \subseteq G$, in der U ein Normalteiler ist, bereits $H \subseteq N_G(U)$ erfüllt.
(3) Bestimmen Sie $N_G(U)$ für die Untergruppe $U := \langle (1,2) \rangle$ der symmetrischen Gruppe $G := \mathcal{S}_3$ auf der Menge $\{1,2,3\}$.
(4) Es sei $p \in \mathbb{P}$ eine Primzahl, die $|G|$ teilt, und $S \in \mathrm{Syl}_p(G)$ eine Sylow-p-Untergruppe von G. Zeigen Sie die Äquivalenz der folgenden Aussagen.
   (a) Es gilt $N_G(S) = G$.
   (b) Es gilt $\mathrm{Syl}_p(G) = \{S\}$.

Lösung:

(1) Es gilt $eUe^{-1} = eUe = U$ und damit ist $e \in U$. Sind $g, h \in N_G(U)$ so gilt

$$(gh)U(gh)^{-1} = (gh)U(h^{-1}g^{-1}) = g(hUh^{-1})g^{-1} \overset{h \in N_G(U)}{=} gUg^{-1} \overset{g \in N_G(U)}{=} U.$$

Damit gilt $gh \in N_G(U)$. Weiter ist

$$g^{-1}U(g^{-1})^{-1} = g^{-1}Ug \overset{g \in N_G(U)}{=} g^{-1}(gUg^{-1})g = (g^{-1}g)U(g^{-1}g) = eUe = U.$$

Damit gilt $g^{-1} \in N_G(U)$. Das Untergruppenkriterium liefert die Behauptung.

Weiter gilt für $u \in U$ die Gleichung $uUu^{-1} = U$ und damit $u \in N_G(U)$. Insgesamt also $U \subseteq N_G(U)$.

(2) Es gilt nach Definition $gUg^{-1} = U$ für alle $g \in N_G(U)$. Damit ist U ein Normalteiler von $N_G(U)$. Es sei H wie in der Voraussetzung und $h \in H$. Da U normal in H ist gilt $hUh^{-1} = U$ und damit $h \in N_G(U)$. Also $H \subseteq N_G(U)$.

(3) Wir geben zwei mögliche Lösungen.
- Es gilt $U = \{\mathrm{id}, (1,2)\}$, da $\mathrm{ord}((1,2)) = 2$ gilt. Für $\sigma \in \mathcal{S}_3$ gilt nun
$$\sigma U \sigma^{-1} = \{\sigma \circ \mathrm{id} \circ \sigma^{-1}, \sigma \circ (1,2) \circ \sigma^{-1}\} = \{\mathrm{id}, (\sigma(1), \sigma(2))\}.$$
Damit gilt
$$\sigma \in N_G(U) \Leftrightarrow \sigma U \sigma^{-1} = U \Leftrightarrow (\sigma(1), \sigma(2)) = (1,2) \Leftrightarrow \{\sigma(1), \sigma(2)\} = \{1,2\}.$$
Gilt $\sigma(1) = 1$ und $\sigma(2) = 2$, so ist $\sigma(3) = 3$ und $\sigma = \mathrm{id}$. Im Fall $\sigma(1) = 2$ und $\sigma(2) = 1$ gilt $\sigma = (1,2)$. Das heißt $N_G(U) = \{\mathrm{id}, (1,2)\} = U$.
- Nach (2) gilt $U \subseteq N_G(U) \subseteq G$. Zweifache Anwendung des Satzes von Lagrange liefert $2 = |U| \mid |N_G(U)|$ und $|N_G(U)| \mid |\mathcal{S}_3| = 6$. Das heißt $|N_G(U)| \in \{2, 6\}$, da $6 = 2 \cdot 3$. Es gilt $(1,3)U(1,3)^{-1} = \{\mathrm{id}, (1,3) \circ (1,2) \circ (1,3)^{-1}\} =$

$\{\mathrm{id}, (2,3)\} \neq U$. Damit gilt $U \neq G$ und $|N_G(U)| \neq 6$. Also $|N_G(U)| = 2$ und $U \subseteq N_G(U)$ liefert $U = N_G(U)$.

(4) (a) $\Rightarrow$ (b). Es sei $N_G(S) = G$. Nach (2) ist damit S ein Normalteiler von G. Nach Vorlesung (Korollar 2.2.2) gilt damit $\mathrm{Syl}_p(G) = \{S\}$.

(b) $\Rightarrow$ (a). Es gelte $\mathrm{Syl}_p(G) = \{S\}$. Nach Korollar 2.2.2 ist damit S ein Normalteiler von G. Nach (2) gilt damit $G \subseteq N_G(S)$ und damit $G = N_G(S)$.

Aufgabe 4. (3+3+2+2 Punkte) Wir betrachten den Körper $K := \mathbb{Z}/(3)$ mit 3 Elementen. Der Übersicht halber schreiben wir in dieser Aufgabe $K = \{0, 1, 2\}$ anstatt $\{0 + (3), 1 + (3), 2 + (3)\}$. Es gilt also z.B. $1 + 2 = 0$ und $2 \cdot 2 = 1$. Es ist

$$G := \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \mid a, c, d \in K, a \neq 0 \neq d \right\} \subseteq \mathrm{GL}_2(K)$$

eine Untergruppe der invertierbaren (2×2)-Matrizen mit Koeffizienten in K. Sie dürfen ohne Beweis verwenden, dass $|G| = 12$ gilt.

(1) Zeigen Sie, dass G auf der Menge $X := \{(u, v) \mid u, v \in K\}$ durch

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} .(u, v) := (a \cdot u, c \cdot u + d \cdot v) \text{ für alle } \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in G, (u, v) \in X$$

operiert.

(2) Es sei $x := (1, 1) \in X$. Bestimmen Sie den Stabilisator $G_x \subseteq G$ und zeigen Sie, dass $|G.x| = 6$ gilt.

(3) Bestimmen Sie die Menge der Fixpunkte X^G.

(4) Entscheiden Sie, ob ein Element $y \in X$ mit $|G.y| = 2$ existiert.

Lösung:

(1) Es seien $g_1 = \begin{pmatrix} a_1 & 0 \\ c_1 & d_1 \end{pmatrix}, g_2 = \begin{pmatrix} a_2 & 0 \\ c_2 & d_2 \end{pmatrix}$ und $(u, v) \in X$. Es gilt

$$\begin{aligned} g_1.(g_2.(u, v)) &= g_1.(a_2 \cdot u, c_2 \cdot u + d_2 \cdot v) \\ &= (a_1 \cdot a_2 \cdot u, c_1 \cdot a_2 \cdot u + d_1 \cdot (c_2 \cdot u + d_2 \cdot v)) \\ &= ((a_1 \cdot a_2) \cdot u, (c_1 \cdot a_2 + d_1 \cdot c_2) \cdot u + (d_1 \cdot d_2) \cdot v) \\ &= (g_1 g_2).(u, v), \end{aligned}$$

da

$$g_1 g_2 = \begin{pmatrix} a_1 & 0 \\ c_1 & d_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & 0 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 \cdot a_2 & 0 \\ c_1 \cdot a_2 + d_1 \cdot c_2 & d_1 \cdot d_2 \end{pmatrix}.$$

Weiter gilt $e_G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ mit

$$e_G.(u, v) = (1 \cdot u, 0 \cdot u + 1 \cdot v) = (u, v).$$

Damit handelt es sich um eine Gruppenoperation.

(2) Es sei $g = \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in G$. Es ist g genau dann in G_x, wenn

$$(1,1) = x = g.x = (a \cdot 1, c \cdot 1 + d \cdot 1) = (a, c + d)$$

gilt. Dies ist äquivalent zu $a = 1$ und $c = 1 - d$. Mit $d \in K \setminus \{0\} = \{1, 2\}$ folgt

$$G_x = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} \right\}.$$

Nach der Bahnformel und dem Satz von Lagrange folgt

$$|G.x| = |G/G_x| = \frac{|G|}{|G_x|} = \frac{12}{2} = 6.$$

(3) Für $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in G$ gilt

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}.(0,0) = (a \cdot 0, c \cdot 0 + d \cdot 0) = (0,0).$$

Damit ist $(0,0) \in X^G$. Es sei $z = (r, s) \in X$ ein Fixpunkt. Dann gilt

$$(r, s) = z = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.z = (2 \cdot r, 0 \cdot r + 2 \cdot s) = (r + r, s + s),$$

und damit $r = 0 = s$ und insgesamt $X^G = \{(0,0)\}$.

(4) Nach (2) existiert eine Bahn B_1 der Länge 6. Weiter existiert nach (3) genau eine Bahn B_2 der Länge 1. Da die Bahnen der Operation eine Partition der Menge X bilden und $|X| = 9$ gilt, muss $X \setminus (B_1 \cup B_2)$ mit 2 Elementen auch die Bahn für ein geeignetes $y \in X$ sein.

Die beiden Möglichkeiten für y sind $(0,1)$ und $(0,2)$ mit

$$G.(0,1) = \{(0,1), (0,2)\} = G.(0,2).$$

Dies lässt sich auch direkt nachrechnen, da

$$\begin{aligned} G.(0,1) &= \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix}.(0,1) \;\middle|\; a, c, d \in K, a, d \neq 0 \right\} \\ &= \{(a \cdot 0, c \cdot 0 + d \cdot 1) \mid a, c, d \in K, a, d \neq 0\} \\ &= \{(0, d \cdot 1) \mid a, c, d \in K, a, d \neq 0\} \\ &= \{(0, d) \mid d \in K \setminus \{0\} = \{1, 2\}\} \\ &= \{(0,1), (0,2)\}. \end{aligned}$$

Aufgabe 5. (2+2+3+3 Punkte) Es sei $R \neq \{0\}$ ein kommutativer Ring.

(1) Wann heißen zwei Ideale I, J von R teilerfremd? Geben Sie weiter die Definition eines maximalen Ideals $\mathfrak{m}$ von R an.
(2) Bestimmen Sie $a, b \in \mathbb{Z}$ mit $1 = a \cdot 17 + b \cdot 12$.
(3) Existiert $s \in \mathbb{Z}$ mit $s \equiv 2 \bmod(17)$ und $s \equiv 3 \bmod(12)$? Falls ein solches Element existiert, geben Sie ein solches Element mit Begründung an.
(4) Es seien $S \neq \{0\}$ ein kommutativer Ring, $\varphi\colon R \longrightarrow S$ ein Homomorphismus von Ringen und $\mathfrak{p}$ ein Primideal von S. Zeigen Sie, dass $\varphi^{-1}(\mathfrak{p})$ ein Primideal von R ist. Sie dürfen dabei ohne Beweis verwenden, dass $\varphi^{-1}(\mathfrak{p})$ ein Ideal von R ist.

Lösung:

(1) Zwei Ideale I, J heißen teilerfremd, falls $I + J = R$ gilt. Ein Ideal $\mathfrak{m} \subseteq R$ heißt maximal, falls $\mathfrak{m} \subsetneq R$ gilt und für jedes Ideal $I \subseteq R$ mit $\mathfrak{m} \subsetneq I \subseteq R$ schon $I = R$ gilt.
(2) Wir verwenden den erweiterten euklidischen Algorithmus und erhalten

$$\begin{aligned} 17 &= 1 \cdot 12 + 5 \\ 12 &= 2 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Rückwärtseinsetzen ergibt

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 = 5 - 2 \cdot (12 - 2 \cdot 5) = 5 \cdot 5 - 2 \cdot 12 \\ &= 5 \cdot (17 - 12) - 2 \cdot 12 = 5 \cdot 17 - 7 \cdot 12. \end{aligned}$$

(3) Nach (2) sind 17 und 12 teilerfremd. Damit sind die Ideale (17) und (12) teilerfremd in $\mathbb{Z}$. Damit liefert der chinesische Restsatz einen Isomorphismus von Ringen

$$\varphi\colon \mathbb{Z}/(17 \cdot 12) \longrightarrow \mathbb{Z}/(17) \times \mathbb{Z}/(12)\ ;\ x + (17 \cdot 12) \mapsto (x + (17), x + (12)).$$

Die Elemente $s \in \mathbb{Z}$ mit

$$(2 + (17), 3 + (17)) = \varphi(s + (17 \cdot 12))$$

sind genau die gesuchten Lösungen der Kongruenzgleichungen. Mithilfe von (2) können wir eine solche Lösungen wie folgt konstruieren: Es gilt $1 = 5 \cdot 17 + (-7) \cdot 12$. Wir setzen

$$s := 2 \cdot (-7 \cdot 12) + 3 \cdot (5 \cdot 17).$$

Es gilt

$$s \equiv 2 \cdot (-7 \cdot 12) = 2 \cdot (1 - 5 \cdot 17) \equiv 2 \bmod(17),$$

und

$$s \equiv 3 \cdot (5 \cdot 17) = 3 \cdot (1 + 7 \cdot 12) \equiv 3 \,\mathrm{mod}(12).$$

Damit ist $s = 87$ eine gesuchte Lösung. Die Menge aller Lösungen ist gegeben durch

$$\{87 + z \cdot 204 \mid z \in \mathbb{Z}\}.$$

(4) Es gilt $\varphi(1_R) = 1_S$ nach Definition eines Homomorphismus von Ringen. Da $\mathfrak{p}$ ein Primideal von S ist, gilt nach Definition $\mathfrak{p} \neq S$. Damit gilt $1_S \neq \mathfrak{p}$. Also ist $1_R \notin \varphi^{-1}(\mathfrak{p})$. Damit gilt $\varphi^{-1}(\mathfrak{p}) \neq R$. Es seien $x, y \in R$ mit $xy \in \varphi^{-1}(\mathfrak{p})$. Da φ ein Homomorphismus von Ringen ist, gilt

$$\varphi(x) \cdot \varphi(y) = \varphi(xy) \in \mathfrak{p}.$$

Da $\mathfrak{p}$ ein Primideal von S ist, gilt damit ohne Beschränkung der Allgemeinheit $\varphi(x) \in \mathfrak{p}$ und damit $x \in \varphi^{-1}(\mathfrak{p})$. Damit ist $\varphi^{-1}(\mathfrak{p})$ ein Primideal von R.

Aufgabe 6. (2+2+4+2 Punkte) Es sei

$$R := \{\sum_{i=0}^{n} a_i X^i \in \mathbb{R}[X] \mid n \in \mathbb{N}_0, a_0, \ldots, a_n \in \mathbb{R} \text{ mit } a_1 = 0\} \subseteq \mathbb{R}[X].$$

(1) Zeigen Sie, dass R ein Unterring des Polynomrings $\mathbb{R}[X]$ ist. Sie dürfen dabei voraussetzen, dass $(R, +)$ eine Untergruppe von $\mathbb{R}[X]$ ist.
(2) Zeigen Sie, dass X^3 in R irreduzibel ist. Sie dürfen ohne Beweis verwenden, dass die Einheiten in R genau die Einheiten aus $\mathbb{R}[X]$ sind.
(3) Es sei S ein Integritätsbereich. Geben Sie die Definition eines Primelements s in S an. Zeigen Sie dann, dass X^3 in R kein Primelement ist.
(4) Beweisen Sie die Existenz eines Ideals I von R mit $I \neq (h)$ für alle $h \in R$. Hierbei bezeichnet (h) das von h erzeugte Ideal in R.

Lösung:

(1) Es gilt $1 = 0 \cdot X^1 + 1 \cdot X^0 \in R$. Es seien $f, g \in R$ mit $f = \sum_{i=0}^{n} a_i X^i$ und $g = \sum_{j=0}^{m} b_i X^i$. Wir schreiben $f \cdot g = \sum_{i=0}^{\ell} c_i X^i$. Dann gilt

$$c_1 = a_1 \cdot b_0 + a_0 \cdot b_1 = 0 \cdot b_0 + a_0 \cdot 0 = 0$$

und damit gilt $f \cdot g \in R$. Da $(R, +)$ eine Untergruppe von $\mathbb{R}[X]$ ist, ist damit R ein Unterring von $\mathbb{R}[X]$.

(2) Es gilt $X^3 \notin \mathbb{R} = \mathbb{R}[X]^\times$. Nach Hinweis ist $0 \neq X^3$ damit keine Einheit von R. Es seien $f, g \in R$ mit $X^3 = f \cdot g$. Es folgt aufgrund der Gradformel $3 = \deg(X^3) = \deg(f \cdot g) = \deg(f) + \deg(g)$. Aufgrund von $f, g \in R$ gilt insbesondere $\deg(f), \deg(g) \neq 1$. Damit gilt o.B.d.A. die Gleichung $\deg(f) = 3$ und $\deg(g) = 0$ und damit $g \in \mathbb{R}^\times = \mathbb{R}[X]^\times = R^\times$.

(3) Ein Element $s \in S$ heißt Primelement, falls $s \in S \setminus (\{0\} \cup S^\times)$ gilt und für alle $a, b \in S$ aus $s \mid a \cdot b$ bereits $s \mid a$ oder $p \mid b$ folgt.

Es gilt $X^3 \mid_R X^8$, da $X^5 \in R$. Weiter gilt X^4 und $X^8 = X^4 \cdot X^4$. Die Annahme $X^3 \mid_R X^4$ liefert $f \in R$ mit $f \cdot X^3 = X^4 = X \cdot X^3$, also $(f - X) \cdot X^3 = 0$. Da $R \subseteq \mathbb{R}[X]$ ein Integritätsbereich ist und $X^3 \neq 0$ gilt, folgt damit $X = f \in R$, dies ist ein Widerspruch da $X \notin R$.

(4) Nach (2) und (3) ist X^3 ein irreduzibles Element in R, das kein Primelement ist. Damit ist R nach Vorlesung (Satz 3.4.5) nicht faktoriell und insbesondere kein Hauptidealring (Satz 3.4.2). Also existiert in R ein Ideal, das kein Hauptideal ist.

Aufgabe 7. (3+2+2+3 Punkte) Es sei $\alpha := \sqrt{1+\sqrt{3}} \in \mathbb{R}$.

(1) Es sei $f := 3X^4 - 6X^2 - 6$. Zeigen Sie, dass f irreduzibel in $\mathbb{Q}[X]$ ist. Ist f auch irreduzibel in $\mathbb{Z}[X]$?
(2) Bestimmen Sie den Grad der Körpererweiterung $\mathbb{Q}(\alpha) : \mathbb{Q}$.
(3) Zeigen Sie, dass $\beta := \sqrt{1-\sqrt{3}} \notin \mathbb{Q}(\alpha)$ gilt.
(4) Zeigen Sie, dass $\mathbb{Q}(\alpha) : \mathbb{Q}$ keine normale Erweiterung ist.

Lösung:

(1) Wir definieren $g := X^4 - 2X^2 - 2$. Da g als normiertes Polynom primitiv ist, folgt mit dem Kriterium von Eisenstein für $p = 2$, dass g irreduzibel in $\mathbb{Q}[X]$ und $\mathbb{Z}[X]$ ist. Da 3 eine Einheit in $\mathbb{Q}[X]$ ist, ist damit auch $3g = f$ irreduzibel in $\mathbb{Q}[X]$. Es sind 3 und g keine Einheiten in $\mathbb{Z}[X]$, da $\mathbb{Z}[X]^\times = \mathbb{Z}^\times = \{-1, 1\}$. Damit ist $f = 3g$ in $\mathbb{Z}[X]$ nicht irreduzibel.
(2) Es gilt

$$g(\alpha) = (\sqrt{1+\sqrt{3}})^4 - 2(\sqrt{1+\sqrt{3}})^2 - 2 = 4 + 2\sqrt{3} - 2(1+\sqrt{3}) - 2 = 0.$$

Da g normiert und, wie in (1) gezeigt, irreduzibel ist, ist g das Minimalpolynom von α. Wir erhalten $4 = \deg(g) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$.
(3) Es gilt $1 = \sqrt{1} < \sqrt{3}$. Damit ist $1 - \sqrt{3} < 0$ und $\beta = \sqrt{1-\sqrt{3}} \notin \mathbb{R}$. Mit $\alpha \in \mathbb{R}$ gilt $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$. Damit muss $\beta \notin \mathbb{Q}(\alpha)$ gelten.
(4) Es ist f nach (1) ein irreduzibles Polynom in $\mathbb{Q}[X]$, das in $\mathbb{Q}(\alpha)$ die Nullstelle α besitzt. Weiter ist

$$f(\beta) = 3(\sqrt{1-\sqrt{3}})^4 - 6(\sqrt{1-\sqrt{3}})^2 - 6 = 3(4 - 2\sqrt{3}) - 6(1-\sqrt{3}) - 6 = 0.$$

Damit $\beta \in \mathbb{C}$ eine Nullstelle von f, die nach (3) nicht in $\mathbb{Q}(\alpha) \subseteq \mathbb{C}$ liegt. Damit ist $\mathbb{Q}(\alpha) : \mathbb{Q}$ nach Vorlesung (genauer Satz 5.5.2) nicht normal.