Frühjahr 2022

F22T1A1	F22T1A2	F22T1A3	F22T1A4	F22T1A5
F22T2A1	F22T2A2	F22T2A3	F22T2A4	F22T2A5
F22T3A1	F22T3A2	F22T3A3	F22T3A4	F22T3A5

Herbst 2022

H22T1A1	H22T1A2	H22T1A3	H22T1A4	H22T1A5
H22T2A1	H22T2A2	H22T2A3	H22T2A4	H22T2A5
H22T3A1	H22T3A2	H22T3A3	H22T3A4	H22T3A5

Aufgabe F22T1A1

Sei $A \in \mathcal{M}_{2,\mathbb{Q}}$ eine 2×2-Matrix mit rationalen Einträgen, so dass A^n die Einheitsmatrix I_2 ist für ein $n \geq 1$. Sei $m_A \in \mathbb{Q}[x]$ das Minimalpolynom von A. Zeigen Sie:

(a) Der Grad von m_A ist höchstens 2.

(b) Das Polynom m_A ist ein Teiler von $x^n - 1$ in $\mathbb{Q}[x]$.

(c) Wählt man $n \geq 1$ minimal mit $A^n = I_2$, dann ist $n \in \{1, 2, 3, 4, 6\}$.
Hinweis: Betrachten Sie geeeignete Kreisteilungspolynome.

Lösung:
zu (a) Laut Vorlesung ist jedes Polynom $f \in \mathbb{Q}[x]$ mit $f(A) = 0_{\mathcal{M}_{2,\mathbb{Q}}}$ ein Vielfaches vom Minimalpolynom m_A. Nach dem Satz von Cayley-Hamilton erfüllt das charakteristische Polynom c_A von A die Bedingung $c_A(A) = 0_{\mathcal{M}_{2,\mathbb{Q}}}$, es gilt also $m_A \mid c_A$. Der Grad von c_A stimmt mit der Zeilenanzahl (oder der Spaltenanzahl von A überein, ist also gleich 2. Aus $m_A \mid c_A$ folgt somit $\text{grad}(m_A) \leq 2$.

zu (b) Das Polynom $f = x^n - 1 \in \mathbb{Q}[x]$ erfüllt ebenfalls die Bedingung $f(A) = A^n - I_2 = I_2 - I_2 = 0_{\mathcal{M}_{2,\mathbb{Q}}}$. Daraus folgt, dass m_A ein Teiler von f ist.

zu (c) Sei $n \in \mathbb{N}$ minimal mit $A^n = I_2$. Nach Teil (b) ist das Minimalpolynom $m_A \in \mathbb{Q}[x]$ von A ein Teiler von $x^n - 1$. Weil die irreduziblen Faktoren von $x^n - 1$ in $\mathbb{Q}[x]$ laut Vorlesung die Kreisteilungspolynome Φ_d sind, wobei $d \in \mathbb{N}$ die Teiler von n durchläuft, muss m_A ein Produkt dieser Kreisteilungspolynome sein. Setzen wir $f = x^n - 1$, dann gilt $\text{ggT}(f, f') = \text{ggT}(x^n - 1, nx^{n-1}) = 1$. Das Polynom f besitzt also keine mehrfahren komplexen Nullstellen, und wegen $m_A \mid f$ gilt dasselbe für m_A. Die irreduziblen Faktoren von m_A sind also alle verschieden. Da nach Teil (a) außerdem die Ungleichung $\text{grad}(m_A) \leq 2$ gilt, muss m_A entweder selbst ein Kreisteilungspolynom vom Grad 1 oder 2, oder ein Produkt zweier verschiedener Kreisteilungspolynome vom Grad 1 sein.

Die einzigen linearen Kreisteilungspolynome sind $\Phi_1 = x - 1$ und $\Phi_2 = x + 1$. Im Fall $m_A = \Phi_1$ ist $n = 1$. Im Fall $m_A = \Phi_2$ ist $A + I_2 = 0$, also $A = -I_2 \neq I_2$ und $A^2 = (-I_2)^2 = I_2$, woraus $n = 2$ folgt. Im Fall $m_A = (x - 1)(x + 1) = x^2 - 1$ gilt ebenfalls $n = 2$. Die einzige verbleibende Möglichkeit ist $m_A = \Phi_d$, wobei $d \in \mathbb{N}$ mit $\varphi(d) = \text{grad}(\Phi_d) = 2$ ist. Ist $d = \prod_{i=1}^{r} p_i^{e_i}$ die Primfaktorzerlegung von d (mit $r \in \mathbb{N}$, Primzahlen $p_1, ..., p_r$ und Exponenten $e_1, ..., e_r \in \mathbb{N}$), dann folgt $\prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1) = \varphi(d) = 2$. Dies zeigt, dass $p_i \leq 3$ für alle i gilt, es ist also $d = 2^{e_1} 3^{e_2}$ mt $e_1, e_2 \in \mathbb{N}_0$ und $(e_1, e_2) \neq (0, 0)$. Im Fall $e_1 > 0$, $e_2 = 0$ ist $d = 2^{e_1}$ und $2^{e_1 - 1} = \varphi(d) = 2$, also $e_1 = 2$ und $n = 4$. Im Fall $e_1 = 0$ und $e_2 > 0$ ist $d = 3^{e_1}$ und $2 \cdot 3^{e_2 - 1} = \varphi(d) = 2$, also $e_2 = 1$ und $n = 3$. Im Fall $e_1, e_2 > 0$ schließlich erhalten wir $2^{e_1 - 1} \cdot 2 \cdot 3^{e_2 - 1} = 2^{e_1} 3^{e_2 - 1} = \varphi(d) = 2$, was nur für $(e_1, e_2) = (1, 1)$ und $n = 6$ möglich ist. Insgesamt ist damit $n \in \{1, 2, 3, 4, 6\}$ nachgewiesen.

Aufgabe F22T1A2

(a) Bestimmen Sie die letzten drei Ziffern von 7^{404404}.

(b) Es sei φ die Eulersche φ-Funktion. Zeigen Sie, dass $\varphi(n^2) = n\varphi(n)$ für alle $n \in \mathbb{N}$ gilt.

(c) Es sei p eine Primzahl mit $p \notin \{2, 5\}$. Zeigen Sie, dass p eine der Zahlen 9, 99, 999, 9999, ... teilt.

Lösung:
zu (a) Die letzten drei Ziffern einer natürlichen Zahl in Dezimaldarstellung hängen nur von der Restklasse der Zahl modulo 1000 ab. Es genügt deshalb, das Bild von $n = 7^{404404}$ in $\mathbb{Z}/1000\mathbb{Z}$ zu bestimmen. Mit 7 ist auch n teilerfremd zu 1000, also ist $\bar{n} = n + 1000\mathbb{Z}$ ein Element von $(\mathbb{Z}/1000\mathbb{Z})^\times$. Die Ordnung der primen Restklassengruppe $(\mathbb{Z}/1000\mathbb{Z})^\times$ ist $\varphi(1000) = \varphi(8)\varphi(125) = 4 \cdot 100$. Daraus folgt $7^{400} = 1$. Wegen $404404 \equiv 4 \bmod 400$ existiert ein $m \in \mathbb{N}$ mit $404404 = 400m + 4$. Damit erhalten wir $\bar{n} = \bar{7}^{404404} = \bar{7}^{400m+4} = (\bar{7}^{400})^m \cdot \bar{7}^4 = \bar{1}^m \cdot \bar{7}^4 = \overline{49}^2 = \overline{2401} = \overline{401}$. Dies zeigt, dass 4, 0 und 1 die letzten drei Ziffern von n sind.

zu (b) Sei $n = \prod_{i=1}^{r} p_i^{e_i}$ die Primfaktorzerlegung von n, mit $r \in \mathbb{N}_0$, Primzahlen $p_1, ..., p_r$ und $e_1, ..., e_r \in \mathbb{N}$. Dann gilt

$$\begin{aligned}\varphi(n^2) &= \varphi\left(\prod_{i=1}^{r} p_i^{2e_i}\right) = \prod_{i=1}^{r} \varphi(p_i^{2e_i}) = \prod_{i=1}^{r} p_i^{2e_i-1}(p_i-1) = \prod_{i=1}^{r} p_i^{e_i} p_i^{e_i-1}(p_i-1) \\ &= \prod_{i=1}^{r} p_i^{e_i} \cdot \prod_{i=1}^{r} p_i^{e_i-1}(p_i-1) = \prod_{i=1}^{r} p_i^{e_i} \cdot \prod_{i=1}^{r} \varphi(p_i^{e_i}) = n\varphi(n).\end{aligned}$$

zu (c) Als Primzahl ungleich 2 und 5 ist p teilerfremd zu 10. Dies zeigt, dass $\overline{10} = 10 + p\mathbb{Z}$ in der primen Restklassengruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ ist. Da es sich dabei um eine endliche Gruppe handelt, besitzt das Element $\overline{10}$ eine endliche Ordnung. Es existiert also ein $m \in \mathbb{N}$ mit $\overline{10}^m = \bar{1}$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. Daraus wiederum folgt $10^m \equiv 1 \bmod p$, was zu $p \mid (10^m - 1)$ äquivalent ist. Die Primzahl p ist also ein Teiler von $10^m - 1 = 99....99$, der Zahl, deren Dezimaldarstellung aus genau m-mal der Ziffer „9“ besteht.

Beispiel: Sei $p = 61$. Dann hat $\overline{10} = 10 + 61\mathbb{Z}$ in $(\mathbb{Z}/61\mathbb{Z})^\times$ die Ordnung 60. Dies zeigt, dass 61 ein Teiler von

$$10^{60} - 1 = 999999999999999999999999999999999999999999999999999999999999 \quad \text{ist.}$$

Aufgabe F22T1A3

Man betrachte die symmetrische Gruppe S_4 des Grades 4 und

$$V \quad = \quad \{\mathrm{id}\ ,\ (1\ 2)(3\ 4)\ ,\ (1\ 3)(2\ 4)\ ,\ (1\ 4)(2\ 3)\} \quad \subseteq \quad S_4.$$

(a) Zeigen Sie, dass V ein zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ isomorpher Normalteiler in S_4 ist.

(b) Zeigen Sie, dass S_4/V zu S_3 isomorph ist.

(c) Beweisen Sie, dass S_4 keinen Normalteiler der Ordnung 8 hat.

(d) Bestimmen Sie alle Untergruppen und alle Normalteiler der Faktorgruppe S_4/V.

Lösung:
zu (a) Zunächst zeigen wir, dass V eine Untergruppe von S_4 ist. Das Neutralelement id von S_4 ist in V enthalten. Seien nun $\sigma, \tau \in V$ vorgegeben; zu zeigen ist $\sigma \circ \tau \in V$ und $\sigma^{-1} \in V$. Wie man leicht überprüft, gilt $\rho^2 = \mathrm{id}$ für alle $\rho \in V$. Daraus folgt, dass jedes Element in V sein eigenes Inverses ist und insbesondere $\sigma^{-1} = \sigma$ in V liegt. Ist $\sigma = \mathrm{id}$, dann folgt $\sigma \circ \tau = \tau$, und dieses Element ist in V enthalten. Ist $\tau = \mathrm{id}$, dann gilt $\sigma \circ \tau = \sigma$ und somit ebenfalls $\sigma \circ \tau \in V$. Im Fall $\sigma, \tau \neq \mathrm{id}$ zeigt die folgende Verknüpfungstabelle, dass $\sigma \circ \tau$ in V enthalten ist.

$\circ$	$(1\ 2)(3\ 4)$	$(1\ 3)(2\ 4)$	$(1\ 4)(2\ 3)$
$(1\ 2)(3\ 4)$	id	$(1\ 4)(2\ 3)$	$(1\ 3)(2\ 4)$
$(1\ 3)(2\ 4)$	$(1\ 4)(2\ 3)$	id	$(1\ 2)(3\ 4)$
$(1\ 4)(2\ 3)$	$(1\ 3)(2\ 4)$	$(1\ 2)(3\ 4)$	id

Als Gruppe der Primzahlquadratordnung 4 ist V abelsch. Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen ist V isomorph zu einem direkten Produkt zyklischer Gruppen, also isomorph zu $\mathbb{Z}/4\mathbb{Z}$ oder $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Da jedes Element in V sein eigenes Inverses ist, gibt es in V nur Elemente der Ordnung 1 und 2, und folglich ist V isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Nun zeigen wir noch, dass V ein Normalteiler von S_4 ist. Laut Vorlesung sind zwei Elemente in S_4 genau dann zueinander konjugiert, wenn sie denselben Zerlegungstyp besitzen. Die drei Elemente $\neq \mathrm{id}$ in V sind die einzigen Doppeltranspositionen in S_4, also die einzigen Elemente vom Zerlegungstyp $(2,2)$. Seien nun $\sigma \in S_4$ und $\tau \in V$ vorgegeben; zu zeigen ist $\sigma \circ \tau \circ \sigma^{-1} \in V$. Ist $\tau \in V \setminus \{\mathrm{id}\}$, dann ist mit τ auch das zu τ konjugierte Element $\sigma \circ \tau \circ \sigma^{-1}$ eine Doppeltransposition, und es folgt $\sigma \circ \tau \circ \sigma^{-1} \in V$. Im Fall $\tau = \mathrm{id}$, ist $\sigma \circ \tau \circ \sigma^{-1}$ gleich id und somit ebenfalls in V enthalten.

zu (b) Sei $X = V \setminus \{\mathrm{id}\}$. Wie wir in Teil (a) gesehen haben, ist mit $\sigma \in S_4$ und $\tau \in X$ auch $\sigma \circ \tau \circ \sigma^{-1}$ wieder in X enthalten. Durch $(\sigma, \tau) \mapsto \sigma \circ \tau \circ \sigma^{-1}$ ist also eine Abbildung $\cdot : S_4 \times X \to X$ definiert. Dabei handelt es sich um eine Gruppenoperation von S_4 auf X. Sind nämlich $\sigma_1, \sigma_2 \in S_4$ und $\tau \in X$ vorgegeben, dann gilt $\mathrm{id} \cdot \tau = \tau \circ \mathrm{id} \circ \tau^{-1} = \tau \circ \tau^{-1} = \mathrm{id}$ und

$$\begin{aligned} \sigma_1 \cdot (\sigma_2 \cdot \tau) \quad &= \quad \sigma_1 \cdot (\sigma_2 \circ \tau \circ \sigma_2^{-1}) \quad = \quad \sigma_1 \circ (\sigma_2 \circ \tau \circ \sigma_2^{-1}) \circ \sigma_1^{-1} \quad = \\ &(\sigma_1 \circ \sigma_2) \circ \tau \circ (\sigma_1 \circ \sigma_2)^{-1} \quad = \quad (\sigma_1 \circ \sigma_2) \cdot \tau. \end{aligned}$$

Laut Vorlesung erhält man durch die Operation einen Gruppenhomomorphismus $\phi : S_4 \to \mathrm{Per}(X)$, definiert durch $\phi(\sigma)(\tau) = \sigma \cdot \tau = \sigma \circ \tau \circ \sigma^{-1}$. Dabei ist V im Kern von ϕ enthalten, denn weil V abelsch ist, gilt für alle $\sigma, \tau \in V$ jeweils $\phi(\sigma)(\tau) = \sigma \circ \tau \circ \sigma^{-1} = \sigma \circ \sigma^{-1} \circ \tau$, und somit $\phi(\sigma) = \mathrm{id}_X$ für alle $\sigma \in V$. Somit induziert ϕ einen Homomorphismus $\bar{\phi} : S_4/V \to \mathrm{Per}(X)$.

Wenn wir zeigen können, dass $\bar{\phi}$ surjektiv ist, dass folgt daraus direkt, dass $S_4/V \cong S_3$ gilt. Denn wegen $|X| = 3$ gilt $\mathrm{Per}(X) \cong S_3$ und somit $|\mathrm{Per}(X)| = |S_3| = 6$. Ebenso ist $|S_4/V| = (S_4 : V) = \frac{|S_4|}{|V|} = \frac{24}{4} = 6$, und als surjektive Abbildung zwischen gleichmächtigen Mengen ist $\bar{\phi}$ auch bijektiv. Insgesamt ist $\bar{\phi}$ also ein Isomorphismus, und es folgt $S_4/V \cong \mathrm{Per}(X) \cong S_3$.

Beweisen wir also noch die Surjektivität von $\bar{\phi}$. Das Element $(1\ 2\ 3) \in S_4$ ist ein Element der Ordnung 3, also muss die Ordnung von $\bar{\phi}((1\ 2\ 3))$ gleich 1 oder 3 sein. Wegen $\phi((1\ 2\ 3))((1\ 2)(3\ 4)) = (1\ 2\ 3) \circ (1\ 2)(3\ 4) \circ (1\ 2\ 3)^{-1} = (1\ 2\ 3) \circ (1\ 2)(3\ 4) \circ (1\ 3\ 2) = (1\ 4)(2\ 3) \neq (1\ 2)(3\ 4)$ ist $\phi((1\ 2\ 3)) \neq \mathrm{id}$ und somit ein Element der Ordnung 3 in $\mathrm{Per}(X)$. Ebenso zeigt die Rechung $\bar{\phi}((1\ 2))((1\ 3)(2\ 4)) = (1\ 2) \circ (1\ 3)(2\ 4) \circ (1\ 2)^{-1} = (1\ 2) \circ (1\ 3)(2\ 4) \circ (1\ 2) = (1\ 4)(2\ 3) \neq (1\ 3)(2\ 4)$, dass $\phi((1\ 2))$ in $\mathrm{Per}(X)$ ein Element der Ordnung 2 ist. Die Ordnung des Bildes $\mathrm{im}(\bar{\phi})$ muss also ein gemeinsames Vielfaches von 2 und 3 sein. Aus $|\mathrm{im}(\bar{\phi})| \geq \mathrm{kgV}(2,3) = 6 = |\mathrm{Per}(X)|$ und $\mathrm{im}(\bar{\phi}) \subseteq \mathrm{Per}(X)$ folgt $\mathrm{im}(\bar{\phi}) = \mathrm{Per}(X)$ und somit die Surjektivität von $\bar{\phi}$.

Anmerkung:
Setzt man als bekannt voraus, dass S_3 bis auf Isomorphie die einzige nicht-abelsche Gruppe der Ordnung 6 ist, kommt man schneller zum Ziel. Wie oben zeigt man zunächst, dass auch die Faktorgruppe S_4/V von Ordnung 6 ist. Anschließend überprüft man noch, dass S_4/V nicht-abelsch ist, zum Beispiel, indem man nachrechnet, dass

$$(1\ 2)V \cdot (1\ 3)V \quad \neq \quad (1\ 3)V \cdot (1\ 2)V$$

gilt. Das Element auf der linken Seite ist gleich $((1\ 2) \circ (1\ 3))V = (1\ 3\ 2)V$, das auf der rechten Seite ist gleich $((1\ 3) \circ (1\ 2))V = (1\ 2\ 3)V$. Wären die Elemente gleich dann müsste $(1\ 3\ 2)^{-1} \circ (1\ 2\ 3)$ in V liegen. Tatsächlich aber gilt $(1\ 3\ 2)^{-1} \circ (1\ 2\ 3) = (1\ 2\ 3) \circ (1\ 2\ 3) = (1\ 3\ 2) \notin V$.

zu (c) Wegen $|S_4| = 24 = 2^3 \cdot 3$ sind die Untergruppen der Ordnung 8 genau die 2-Sylowgruppen von S_4. Gäbe es eine 2-Sylowgruppe, die Normalteiler ist, so wäre dies laut Zweitem Sylowsatz die einzige 2-Sylowgruppe. Nun ist bekanntlich die Diedergruppe D_4 eine Untergruppe der Ordnung 8 von S_4, und diese enthält zwei Elemente der Ordnung 4. Wäre dies die einzige Untergruppe der Ordnung 8, dann gäbe es also nur zwei Elemente der Ordnung 4 in S_4. Offensichtlich gibt es aber mehr als zwei solche Elemente, zum Beispiel (1 2 3 4), (1 4 3 2) und (1 3 2 4).

zu (d) Nach Teil (b) ist S_4/V isomorph zu S_3. Bekanntlich besitzt S_3 genau drei verschiedene Untergruppen der Ordnung 2 und genau je eine Untergruppe der Ordnung 1, 3 und 6. Dabei sind die drei Untergruppen der Ordnung 2 keine Normalteiler, die übrigen drei Gruppen sind Normalteiler. Auf Grund der Isomorphie besitzt S_4/V die gleiche Untergruppenstruktur.

Das Neutralelement von S_4/V ist $e_{S_4/V} = V$, und offenbar ist $\{V\}$ die eindeutig bestimmte Untergruppe der Ordnung 1 von S_4/V. Ebenso ist S_4/V die eindeutig bestimmte Untergruppe der Ordnung 6 von S_4/V. Wir betrachten in S_4/V nun die Elemente $g_1 = (1\ 2)V$, $g_2 = (1\ 3)V$, $g_3 = (1\ 4)V$ und $h = (1\ 2\ 3)V$. Wegen $(1\ 2), (1\ 3), (1\ 4) \notin V$ gilt $g_1 \neq e_{S_4/V}$, $g_2 \neq e_{S_4/V}$ und $g_3 \neq e_{S_4/V}$. Andererseits gilt $g_1^2 = (1\ 2)^2V = \mathrm{id}V = e_{S_4/V}$, also ist g_1 in S_4/V ein Element der Ordnung 2. Ebenso zeigen die Gleichungen $g_2^2 = (1\ 3)^2V = \mathrm{id}V = e_{S_4/V}$ und $g_3^2 = (1\ 4)^2V = \mathrm{id}V = e_{S_4/V}$, dass auch g_2 und g_3 Elemente der Ordnung 2 in S_4/V sind.

Durch $\langle g_1 \rangle = \{e_{S_4/V}, g_1\}$, $\langle g_2 \rangle = \{e_{S_4/V}, g_2\}$ und $\langle g_3 \rangle = \{e_{S_4/V}, g_3\}$ sind also Untergruppen von S_4/V der Ordnung 2 gegeben. Würden zwei davon übereinstimmen, dann wären auch zwei der Elemente g_1, g_2, g_3 identisch. Aus $g_1 = g_2$ würde $(1\ 2)V = (1\ 3)V$ und $(1\ 2)^{-1} \circ (1\ 3) \in V$ folgen. Aber dies ist wegen $(1\ 2)^{-1} \circ (1\ 3) = (1\ 2) \circ (1\ 3) = (1\ 3\ 2) \notin V$ nicht der Fall. Ebenso zeigen die Rechnungen $(1\ 2)^{-1} \circ (1\ 4) = (1\ 2) \circ (1\ 4) = (1\ 4\ 2) \notin V$ und $(1\ 3)^{-1} \circ (1\ 4) = (1\ 3) \circ (1\ 4) = (1\ 4\ 3) \notin V$, dass $g_1 \neq g_3$ und $g_2 \neq g_3$ gilt. Also sind $\langle g_1 \rangle$, $\langle g_2 \rangle$ und $\langle g_3 \rangle$ die drei Untergruppen der Ordnung 2 von S_4/V.

Es gilt $h = (1\ 2\ 3)V \neq e_{S_4/V}$ wegen $(1\ 2\ 3) \notin V$, $h^2 = (1\ 2\ 3)^2 V = (1\ 3\ 2)V \neq e_{S_4/V}$ wegen $(1\ 3\ 2) \notin V$ und $h^3 = (1\ 2\ 3)^3 V = \mathrm{id}V = e_{S_4/V}$. Also ist $\mathrm{ord}(h) = 3$, und $\langle h \rangle$ ist eine Untergruppe der Ordnung 3 von S_4/V. Insgesamt sind

$$\{V\} \quad , \quad \langle g_1 \rangle \quad , \quad \langle g_2 \rangle \quad , \quad \langle g_3 \rangle \quad , \quad \langle h \rangle \quad \text{und} \quad S_4/V$$

also die sechs Untergruppen von S_4/V, und $\{V\}$, $\langle h \rangle$, S_4/V sind die drei Normalteiler.

Aufgabe F22T1A4

(a) Bestimmen Sie alle Ideale des Rings $R = \mathbb{Z}/2022\mathbb{Z}$. Bestimmen Sie darunter alle Primideale in R.

(b) Bestimmen Sie alle idempotenten Elemente des Rings R, d.h. alle Elemente $a \in R$ mit $a^2 = a$.

(c) Bestimmen Sie die Anzahl der Nullteiler in R.

(d) Bestimmen Sie ein $n \in \mathbb{N}$ mit $n < 2022$ und $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/2022\mathbb{Z})^\times$.

Lösung:
zu (a) Sei $\pi : \mathbb{Z} \to \mathbb{Z}/2022\mathbb{Z}$ der kanonische Epimorphismus und $I = (2022)$. Nach dem Korrespondenzsatz der Ringtheorie ist durch $J \mapsto \pi(J)$ eine Bijektion gegeben zwischen den Idealen J von $\mathbb{Z}$ mit $J \supseteq I$ und den Idealen von $\mathbb{Z}/2022\mathbb{Z}$. Die Ideale von $\mathbb{Z}$ haben alle die Form (n) mit $n \in \mathbb{N}_0$, und es gilt $(n) \supseteq I$ genau dann, wenn 2022 in (n) liegt, was wiederum genau dann der Fall ist, wenn n ein Teiler von 2022 ist. An der Primfaktorzerlegung $2022 = 2 \cdot 3 \cdot 337$ liest man ab, dass 2022 genau acht Teiler in $\mathbb{N}_0$ besitzt, nämlich 1, 2, 3, 6, 337, 674, 1011 und 2022. Die Ideale von $\mathbb{Z}/2022\mathbb{Z}$ sind somit gegeben durch $(\bar{1})$, $(\bar{2})$, $(\bar{3})$, $(\bar{6})$, $(\overline{337})$, $(\overline{674})$, $(\overline{1011})$ und $(\overline{2022}) = (\bar{0}) = \{\bar{0}\}$.

Wir zeigen, dass allgemein gilt: Ist R ein Ring, I ein Ideal von R und $\pi : R \to R/I$ der kanonische Epimorphismus, so ist ein Ideal J von R mit $J \supseteq I$ genau dann ein Primideal, wenn $\pi(J)$ ein Primideal in R/I ist. Ist J ein Primideal, dann gilt zunächst $1_R + I \notin \pi(J)$, denn ansonsten wäre 1_R in $\pi^{-1}(\pi(J)) = J$ enthalten. Sind $a + I, b + I \in R/I$ mit $a, b \in R$ und $(a + I)(b + I) \in \pi(J)$, dann folgt $ab + I \in \pi(J)$ und $ab \in J$. Weil J ein Primideal ist, folgt $a \in J$ oder $b \in J$, und daraus wiederum $a + I \in \pi(J)$ oder $b + I \in \pi(J)$. Also ist $\pi(J)$ ein Primideal in R/I. Setzen wir dies nun umgekehrt voraus, dann ist $1_R \notin J$, denn ansonsten wäre $1_{R/I} = \pi(1_R) \in \pi(J)$. Seien nun $a, b \in R$ mit $ab \in J$. Dann folgt $\pi(a)\pi(b) = \pi(ab) \in \pi(J)$, und daraus wiederum $\pi(a) \in \pi(J)$ oder $\pi(b) \in \pi(J)$, weil $\pi(J)$ ein Primideal ist. Wegen $\pi^{-1}(\pi(J)) = J$ folgt daraus wiederum $a \in J$ oder $b \in J$. Dies zeigt, dass J ein Pprimideal in J ist.

Bekanntlich sind die Primideale in $\mathbb{Z}$ genau das Nullideal und die Ideale der Form (p), wobei p die Primzahlen durchläuft. Die einzigen Primideale, die (2022) enthalten, sind also (2), (3) und (337). Die soeben bewiesene Aussage zeigt, dass $(\bar{2})$, $(\bar{3})$ und $(\overline{337})$ somit die Primideale von $\mathbb{Z}/2022\mathbb{Z}$ sind.

zu (b) Weil $2022 = 2 \cdot 3 \cdot 337$ gilt und die Zahlen 2, 3 und 337 paarweise teilerfremd sind, gilt $\mathbb{Z}/2022\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/337\mathbb{Z}$ nach dem Chinesischen Restsatz. Ein Element $(\bar{a}, \bar{b}, \bar{c}) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/337\mathbb{Z}$ ist genau dann idempotent, wenn $(\bar{a}^2, \bar{b}^2, \bar{c}^2) = (\bar{a}, \bar{b}, \bar{c})^2 = (\bar{a}, \bar{b}, \bar{c})$ gilt, was wiederum zu $\bar{a}^2 = \bar{a}$, $\bar{b}^2 = \bar{b}$ und $\bar{c}^2 = \bar{c}$ ist. Nun ist in einem Körper K für jedes $\alpha \in K$ die Gleichung $\alpha^2 = \alpha$ äquivalent zu $\alpha(\alpha - 1_K) = 0_K$ und damit zu $\alpha \in \{0_K, 1_K\}$. Weil 2, 3 und 337 Primzahlen sind, sind $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ und $\mathbb{Z}/337\mathbb{Z}$ Körper. Also sind die Gleichungen $\bar{a}^2 = \bar{a}$, $\bar{b}^2 = \bar{b}$, $\bar{c}^2 = \bar{c}$ äquivalent zu $\bar{a} \in \{\bar{0}, \bar{1}\}$, $\bar{b} \in \{\bar{0}, \bar{1}\}$, $\bar{c} \in \{\bar{0}, \bar{1}\}$. Insgesamt zeigt dies, dass in $\mathbb{Z}/2022\mathbb{Z}$ genau acht idempotente Elemente existieren, nämlich die Urbilder von

$$(\bar{0}, \bar{0}, \bar{0}), (\bar{0}, \bar{0}, \bar{1}), (\bar{0}, \bar{1}, \bar{0}), (\bar{0}, \bar{1}, \bar{1}), (\bar{1}, \bar{0}, \bar{0}), (\bar{1}, \bar{0}, \bar{1}), (\bar{1}, \bar{1}, \bar{0}), (\bar{1}, \bar{0}, \bar{1})$$

unter dem Isomorphismus $\mathbb{Z}/2022\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/337\mathbb{Z}$. Wir rechnen diese acht Urbilder nun aus. Das Urbild von $(\bar{0}, \bar{0}, \bar{0})$ ist das eindeutig bestimmte Element $a + 2022\mathbb{Z}$ mit $a \equiv 0 \bmod 2$, $a \equiv 0 \bmod 3$ und $a \equiv 0 \bmod 337$, und dies ist offenbar $0 + 2022\mathbb{Z}$. Genauso sieht man, dass $1 + 2022\mathbb{Z}$ das Urbild von $(\bar{1}, \bar{1}, \bar{1})$ ist.

Das Urbild $a + 2022\mathbb{Z}$ von $(\bar{0}, \bar{0}, \bar{1})$ erfüllt $a \equiv 0 \bmod 2$, $a \equiv 0 \bmod 3$ und $a \equiv 1 \bmod 337$, was äquivalent ist zu $a \equiv 0 \bmod 6$ und $a \equiv 1 \bmod 337$. Die letzte Bedingung zeigt, dass a die Form $1 + 337k$ mit $k \in \mathbb{Z}$ haben muss. Wegen $337 \equiv 1 \bmod 6$ erfüllt $1 + 337 \cdot 5 = 1686$ auch die Bedingung $1686 \equiv 0 \bmod 6$. Also ist $1686 + 2022\mathbb{Z}$ das Ubild von $(\bar{0}, \bar{0}, \bar{1})$.

Das Urbild $a + 2022\mathbb{Z}$ von $(\bar{0}, \bar{1}, \bar{0})$ erfüllt $a \equiv 0 \bmod 2$, $a \equiv 1 \bmod 3$ und $a \equiv 0 \bmod 337$, was äquivalent ist zu $a \equiv 0 \bmod 674$ und $a \equiv 1 \bmod 3$. Es gilt $674 \equiv 2 \bmod 3$, also $1348 \equiv 2 \cdot 674 \equiv 4 \equiv 1 \bmod 3$. Also ist $1348 + 2022\mathbb{Z}$ das Urbild von $(\bar{0}, \bar{1}, \bar{0})$. Durch analoge Rechnungen sieht man, dass die Urbilder von $(\bar{0}, \bar{1}, \bar{1}), (\bar{1}, \bar{0}, \bar{0}), (\bar{1}, \bar{0}, \bar{1})$ und $(\bar{1}, \bar{1}, \bar{0})$ durch $1012 + 2022\mathbb{Z}$, $1011 + 2022\mathbb{Z}$, $675 + 2022\mathbb{Z}$ und $337 + 2022\mathbb{Z}$ gegeben sind. Die idempotenten Elemente von $\mathbb{Z}/2022\mathbb{Z}$ sind also $a + 2022\mathbb{Z}$ mit $a \in \{0, 1, 337, 675, 1011, 1012, 1348, 1686\}$.

zu (c) Weil $\mathbb{Z}/2022\mathbb{Z}$ ein endlicher Ring ist, ist jedes Element entweder Einheit oder Nullteiler. Laut Vorlesung hat die Einheitengruppe $(\mathbb{Z}/2022\mathbb{Z})^\times$ die Ordnung $\varphi(2022) = \varphi(2)\varphi(3)\varphi(337) = 1 \cdot 2 \cdot 336 = 772$. Die Zahl der Nullteiler ist also gegeben durch $|\mathbb{Z}/2022\mathbb{Z}| - |(\mathbb{Z}/2022\mathbb{Z})^\times| = 2022 - 772 = 1350$.

zu (d) Sei $n = 1011$; diese Zahl besitzt die Primfaktorzerlegung $3 \cdot 337$. Wegen $(\mathbb{Z}/2\mathbb{Z})^\times = \{\bar{1}\}$ und dem Chinesischen Restsatz gilt

$$\begin{aligned}(\mathbb{Z}/n\mathbb{Z})^\times \quad &\cong \quad (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/337\mathbb{Z})^\times \quad \cong \quad \{\bar{1}\} \times (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/337\mathbb{Z})^\times \\ &\cong \quad (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/337\mathbb{Z})^\times \quad \cong \quad (\mathbb{Z}/2022\mathbb{Z})^\times.\end{aligned}$$

Aufgabe F22T1A5

Für jedes $n \in \mathbb{N}$ sei $a_n = \sqrt[2^n]{2}$. Weiter seien $A = \{a_n \mid n \in \mathbb{N}\}$ und $K = \mathbb{Q}(A)$. Zeigen Sie:

(a) $[\mathbb{Q}(a_n) : \mathbb{Q}] = 2^n$ für jedes $n \in \mathbb{N}$

(b) $[K : \mathbb{Q}] = \infty$

(c) $K = \bigcup_{n\in\mathbb{N}} \mathbb{Q}(a_n)$

(d) K ist eine algebraische Erweiterung von $\mathbb{Q}$

Lösung:
zu (a) Das Polynom $f_n = x^{2^n} - 2 \in \mathbb{Z}[x]$ ist normiert, nach dem Eisenstein-Kriterium (angewendet auf die Primzahl 2) über $\mathbb{Q}$ irreduzibel, und es gilt $f_n(a_n) = (\sqrt[2^n]{2})^{2^n} - 2 = 2 - 2 = 0$. Somit ist f_n das Minimalpolynom von a_n über $\mathbb{Q}$, und es folgt $[\mathbb{Q}(a_n) : \mathbb{Q}] = \operatorname{grad}(f_n) = 2^n$.

zu (b) Nehmen wir an, der Grad $m = [K : \mathbb{Q}]$ wäre endlich. Wegen $a_n \in A \subseteq \mathbb{Q}(A) = K$ ist $\mathbb{Q}(a_n)$ für jedes $n \in \mathbb{N}$ ein Zwischenkörper von $K|\mathbb{Q}$. Mit der Gradformel und dem Ergebnis von Teil (a) erhalten wir

$$m \quad = \quad [K : \mathbb{Q}] \quad = \quad [K : \mathbb{Q}(a_n)] \cdot [\mathbb{Q}(a_n) : \mathbb{Q}] \quad = \quad [K : \mathbb{Q}(a_n)] \cdot 2^n$$

für alle $n \in \mathbb{N}$. Die Zahl $m \in \mathbb{N}$ wäre also durch 2^n teilbar für jedes $n \in \mathbb{N}$, was offenbar unmöglich ist.

zu (c) „$\supseteq$“ Wie bereits in Teil (b) festgestellt, ist $\mathbb{Q}(a_n)$ für jedes $n \in \mathbb{N}$ ein Zwischenkörper von $K|\mathbb{Q}$. Insbesondere gilt also $\mathbb{Q}(a_n) \subseteq K$ für alle $n \in \mathbb{N}$, und damit auch $\bigcup_{n\in\mathbb{N}} \mathbb{Q}(a_n) \subseteq K$. „$\subseteq$“ Sei $L = \bigcup_{n\in\mathbb{N}} \mathbb{Q}(a_n)$. Für jedes $m \in \mathbb{N}$ gilt $a_m \in \mathbb{Q}(a_m) \subseteq L$ und damit $A = \{a_m \mid m \in \mathbb{N}\} \subseteq L$.

Außerdem ist L ein Zwischenkörper der Erweiterung $\mathbb{R}|\mathbb{Q}$. Zum Nachweis der Teilkörper-Eigenschaft stellen wir zunächst fest, dass 1 in $\mathbb{Q}(a_1) \subseteq L$ enthalten ist. Seien nun $\alpha, \beta \in L$ vorgegeben. Dann gibt es nach Definition von L natürliche Zahlen m, n mit $\alpha \in \mathbb{Q}(a_m)$ und $\beta \in \mathbb{Q}(a_n)$. Nach eventueller Vertauschung von α und β können wir $m \leq n$ annehmen. Wegen $a_m = \sqrt[2^m]{2} = 2^{2^{-m}} = 2^{2^{-n}\cdot 2^{n-m}} = (2^{2^{-n}})^{2^{n-m}} = (\sqrt[2^n]{2})^{2^{n-m}} = a_n^{2^{n-m}} \in \mathbb{Q}(a_n)$ gilt $\mathbb{Q}(a_m) \subseteq \mathbb{Q}(a_n)$. Aus $\alpha \in \mathbb{Q}(a_m) \subseteq \mathbb{Q}(a_n)$ und $\beta \in \mathbb{Q}(a_n)$ sowie der Teilkörper-Eigenschaft von $\mathbb{Q}(a_n)$ folgt nun, dass auch $\alpha - \beta$ und $\alpha\beta$ in $\mathbb{Q}(a_n)$ und wegen $\mathbb{Q}(a_n) \subseteq L$ damit auch in L enthalten sind. Im Fall $\alpha \neq 0$ erhält man ebenso $\alpha^{-1} \in \mathbb{Q}(a_m)$ und damit $\alpha^{-1} \in L$. Damit ist der Nachweis der Teilkörper-Eigenschaft von L abgeschlossen. Außerdem gilt $\mathbb{Q} \subseteq \mathbb{Q}(a_1) \subseteq L$.

Somit ist L tatsächlich ein Zwischenkörper von $\mathbb{R}|\mathbb{Q}$. Da außerdem, wie bereits festgestellt, $A \subseteq L$ gibt, erhalten wir insgesamt $K = \mathbb{Q}(A) \subseteq L$.

zu (d) Es genügt zu zeigen, dass jedes $\alpha \in K$ algebraisch über $\mathbb{Q}$ ist. Sei also $\alpha \in K$ vorgegeben. Auf Grund des Ergebnisses von Teil (c) gilt $\alpha \in \mathbb{Q}(a_n)$ für ein $n \in \mathbb{N}$. Nach Teil (a) ist $\mathbb{Q}(a_n)|\mathbb{Q}$ eine endliche Erweiterung, und jede endliche Erweiterung ist laut Vorlesung algebraisch. Daraus folgt, dass alle Elemente aus $\mathbb{Q}(a_n)$ algebraisch über $\mathbb{Q}$ sind, insbesondere auch das Element α.

alternative Lösung:
Wie wir in Teil (a) festgestellt haben, ist a_n für jedes $n \in \mathbb{N}$ jeweils eine Nullstelle des Polynoms $f_n = x^{2^n} - 1 \in \mathbb{Q}[x]$ und somit algebraisch über $\mathbb{Q}$. Die Menge A besteht also aus Elementen, die algebraisch über $\mathbb{Q}$ sind. Laut Vorlesung ist jede Körpererweiterung, die von Elementen erzeugt wird, die über dem Grundkörper algebraisch sind, selbst eine algebraische Erweiterung. Wegen $K = \mathbb{Q}(A)$ ist die Erweiterung $K|\mathbb{Q}$ somit algebraisch. (Vom Aufgabensteller war aber wohl nicht vorgesehen, dass man dieses Resultat verwendet. Es wird eventuell nicht in jeder Algebra-Vorlesung behandelt.)

Aufgabe F22T2A1

Gegeben sei die komplexe 2×2-Matrix

$$A \quad = \quad \begin{pmatrix} i & 2 \\ 0 & -i \end{pmatrix}.$$

Berechnen Sie die Matrix A^{2022}.

Lösung:
Es gilt

$$A^2 = \begin{pmatrix} i & 2 \\ 0 & -i \end{pmatrix} \begin{pmatrix} i & 2 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{und} \quad A^4 = (A^2)^2 = (-E) = E \quad ,$$

wobei E die 2×2-Einheitsmatrix bezeichnet. Daraus folgt $A^{2022} = A^{4 \cdot 505 + 2} = (A^4)^{505} \cdot A^2 = E^{505} \cdot A^2 = A^2 = -E$.

Aufgabe F22T1A2

(a) Geben Sie eine nicht-abelsche Gruppe der Ordnung 100 an.

(b) Zeigen Sie mit Hilfe der Sylowsätze, dass jede Gruppe der Ordnung 100 auflösbar ist.

(c) Zeigen Sie, dass eine Gruppe der Ordnung 100 genau dann abelsch ist, wenn es in G lediglich eine 2-Sylowgruppe gibt.

Lösung:
zu (a) Laut Vorlesung ist die Diedergruppe D_n für alle $n \in \mathbb{N}$ mit $n \geq 3$ eine nicht-abelsche Gruppe der Ordnung $2n$. Also ist D_{50} eine nicht-abelsche Gruppe der Ordnung 100.

zu (b) Sei G eine Gruppe der Ordnung $100 = 2^2 \cdot 5^2$, und es sei ν_5 die Anzahl der 5-Sylowgruppen von G. Auf Grund des Dritten Sylowsatzes gilt $\nu_5 \mid 2^2$, also $\nu_5 \in \{1, 2, 4\}$, außerdem $\nu_5 \equiv 1 \bmod 5$. Wegen $2, 4 \not\equiv 1 \bmod 5$ folgt daraus $\nu_5 = 1$. Sei N die einzige 5-Sylowgruppe von G. Auf Grund des Zweiten Sylowsatzes ist N ein Normalteiler von G. Als Gruppe der Primzahlpotenzordnung 5^2 ist N eine auflösbare Gruppe. Auch die Ordnung der Faktorgruppe G/N ist eine Primzahlpotenz, nämlich $|G/N| = (G : N) = \frac{|G|}{|N|} = \frac{100}{25} = 2^2$. Somit ist auch G/N auflösbar. Aus der Auflösbarkeit von N und G/N folgt die Auflösbarkeit von G. (Als Gruppen von Primzahlquadratordnung sind N und G/N sogar abelsch, aber daraus folgt natürlich nicht, dass G abelsch sein muss.)

zu (c) Wieder sei G eine Gruppe der Ordnung 100, und für jede Primzahl p sei ν_p die Anzahl der p-Sylowgruppen von G. Bereits in Teil (b) haben wir gesehen, dass G genau eine 5-Sylowgruppe N besitzt, und dass $N \trianglelefteq G$ gilt. Laut Vorlesung besitzt G für jede Primzahl p mindestens eine p-Sylowgruppe. Wir bezeichnen mit U eine beliebige 2-Sylowgruppe und beweisen nun die angegebene Äquivalenz.

„$\Rightarrow$“ Ist G abelsch, dann ist jede Untergruppe von G ein Normalteiler, insbesondere auch die 2-Sylowgruppe U. Aus $U \trianglelefteq G$ folgt auf Grund des Zweiten Sylowsatzes $\nu_2 = 1$. „$\Leftarrow$“ Aus $\nu_2 = 1$ folgt mit dem Zweiten Sylowsatz umgekehrt auch $U \trianglelefteq G$. Wir zeigen nun, dass G ein inneres direktes Produkt von N und U ist. Die Bedingung $N, U \trianglelefteq G$ haben wir bereits verifiziert. Auf Grund der Teilerfremdheit von $|N| = 25$ und $|U| = 4$ gilt $N \cap U = \{e\}$. Für den Nachweis der Gleichung $G = NU$ stellen wir zunächst fest, dass NU wegen $N, U \trianglelefteq G$ eine Untergruppe von G ist (sogar ein Normalteiler). Aus $N \subseteq NU$ folgt mit dem Satz von Lagrange, dass $|N| = 25$ ein Teiler von $|NU|$ ist. Aus $U \subseteq NU$ folgt ebenso $4 \mid |NU|$. Insgesamt ist $|NU|$ damit ein Vielfaches von $\mathrm{kgV}(25, 4) = 100$; insbesondere gilt $|NU| \geq 100 = |G|$. Wegen $NU \subseteq G$ folgt daraus $NU = G$.

Insgesamt ist G also tatsächlich ein inneres direktes Produkt von N und U. Laut Vorlesung folgt daraus $G \cong N \times U$. Als Gruppen von Primzahlquadratordnung sind N und U abelsch. Also ist auch $N \times U$, und auf Grund der Isomorphie auch G, eine abelsche Gruppe.

Aufgabe F22T2A3

Sei $n \in \mathbb{N}$ und R ein kommutativer Ring (mit Einselement). Betrachten Sie für $a, b \in R$ das Ideal $I = (a, b) \subseteq R$.

(a) Zeigen Sie: Aus $a^n = b^n = 0$ folgt $I^{2n} = (0)$.

(b) Nehmen Sie an, dass $2 = 1 + 1$ eine Einheit von R ist und dass $c^2 = 0$ für alle $c \in I$ gilt. Zeigen Sie, dass dann $ab = 0$ folgt.

(c) Geben Sie einen kommutativen Ring R mit Elementen $a, b \in R$ an, für welche $a^2 = b^2 = 0$ und $ab \neq 0$ gilt. Begründen Sie, dass diese beiden Bedingungen für den von Ihnen angegebenen Ring erfüllt sind.
Hinweis: Betrachten Sie $R = \mathbb{Q}[x, y]/I$ für ein geeignetes Ideal I.

Lösung:
zu (a) Wir zeigen durch vollständige Induktion, dass $S_m = \{a^{n-j}b^j \mid 0 \leq j \leq m\}$ für jedes $m \in \mathbb{N}$ ein Erzeugendensystem des Ideals I^m ist. Dass $S_1 = \{a, b\}$ das Ideal $I^1 = I$ erzeugt, gilt laut Angabe. Sei nun $m \in \mathbb{N}$, und setzen wir $I^m = (S_m)$ voraus. Wegen $I^{m+1} = I^m \cdot I$, $I^m = (S_m)$ und $I = (a, b)$ ist laut Vorlesung $S = \{cd \mid c \in S_m, d \in \{a, b\}\}$ ein Erzeugendensystem von I^{m+1}. Diese Menge stimmt mit S_{m+1} überein, denn es gilt

$$\begin{aligned} S &= \{a^{m-j}b^j \cdot a \mid 0 \leq j \leq m\} \cup \{a^{m-j}b^j \cdot b \mid 0 \leq j \leq m\} \\ &= \{a^{m+1-j}b^j \mid 0 \leq j \leq m\} \cup \{a^{(m+1)-(j+1)}b^{j+1} \cdot b \mid 0 \leq j \leq m\} \\ &= \{a^{m+1-j}b^j \mid 0 \leq j \leq m\} \cup \{a^{(m+1)-j}b^j \cdot b \mid 1 \leq j \leq m+1\} \\ &= \{a^{m+1-j}b^j \mid 0 \leq j \leq m+1\} = S_{m+1}. \end{aligned}$$

Setzen wir nun voraus, dass $a^n = b^n = 0$ für ein $n \in \mathbb{N}$ gilt. Für $0 \leq j \leq n$ gilt dann $2n - j \geq n$ und somit $a^{2n-j} \cdot b^j = a^n \cdot a^{n-j} \cdot b^j = 0 \cdot a^{n-j} \cdot b^j = 0$, und für $n < j \leq 2n$ erhalten wir $a^{2n-j} \cdot b^j = a^{2n-j} \cdot b^{j-n} \cdot b^n = a^{2n-j} \cdot b^{j-n} \cdot 0 = 0$. Insgesamt gilt damit $S_{2n} = \{0\}$, und es folgt $I^{2n} = (S_{2n}) = (0)$.

zu (b) Auf Grund der Voraussetzungen gilt $2ab = 0 + 2ab + 0 = a^2 + 2ab + b^2 = (a + b)^2 = 0$. Weil 2 in R eine Einheit ist, folgt daraus $ab = 2^{-1}(2ab) = 2^{-1} \cdot 0 = 0$.

zu (c) Wir betrachten im Polynomring $\mathbb{Q}[x, y]$ das Ideal $I = (x^2, y^2)$ und setzen $R = \mathbb{Q}[x, y]/I$. Es sei $a = x + I$ und $b = y + I$. Wegen $x^2 \in I$ gilt $a^2 = x^2 + I = I = 0_R$, und aus $y^2 \in I$ folgt ebenso $b^2 = y^2 + I = I = 0_R$. Nehmen wir nun an, dass auch $ab = 0_R$ gilt. Dann folgt $xy + I = (x + I)(y + I) = ab = 0_R = I$ und damit $xy \in I$. Nach Definition des Ideals I würden dann Polynome $f, g \in \mathbb{Q}[x, y]$ existieren mit der Eigenschaft, dass die Gleichung $xy = x^2 f + y^2 g$ erfüllt ist. Aber das ist ausgeschlossen, denn stellt man f und g auf der rechten Seite als Summe von Monomen dar, dann kommt weder in $x^2 f$ noch in $y^2 g$ ein Monom vor, dass genau einmal durch x und genau einmal durch y teilbar ist.

Aufgabe F22T2A4

Sei p eine Primzahl und $n \in \mathbb{N}$. Seien $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ endliche Körper mit p bzw. p^n Elementen.

(a) Sei zunächst $n = 2$. Zeigen Sie: Für jedes $a \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ gilt $\mathbb{F}_p(a) = \mathbb{F}_{p^2}$.

(b) Bestimmen Sie die Anzahl der Elemente $a \in \mathbb{F}_{p^2}$ mit $\mathbb{F}_{p^2} = \mathbb{F}_p(a)$.

(c) Sei jetzt $n = 6$. Zeigen Sie, dass die Anzahl der Elemente $a \in \mathbb{F}_{p^6}$ mit $\mathbb{F}_{p^6} = \mathbb{F}_p(a)$ genau $p^6 - p^3 - p^2 + p$ beträgt.

(d) Bestimmen Sie die Anzahl der irreduziblen, normierten Polynome $f \in \mathbb{F}_p[x]$ vom Grad 6.

Lösung:
zu (a) Sei $a \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ vorgegeben. Wegen $a \in \mathbb{F}_{p^2}$ ist $\mathbb{F}_p(a)$ ein Zwischenkörper von $\mathbb{F}_{p^2}|\mathbb{F}_p$. Laut Vorlesung sind die Zwischenkörper dieser Erweiterung durch $\mathbb{F}_{p^d}$ gegeben, wobei $d \in \mathbb{N}$ die Teiler von 2 durchläuft. Es ist somit nur $\mathbb{F}_p(a) = \mathbb{F}_p$ oder $\mathbb{F}_p(a) = \mathbb{F}_{p^2}$ möglich. Im Fall $\mathbb{F}_p(a) = \mathbb{F}_p$ wäre $a \in \mathbb{F}_p$, im Widerspruch zur Voraussetzung. Also muss $\mathbb{F}_p(a) = \mathbb{F}_{p^2}$ gelten.

zu (b) Zunächst zeigen wir, dass umgekehrt aus $\mathbb{F}_{p^2} = \mathbb{F}_p(a)$ auch $a \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ folgt. Auf Grund der Gleichung muss offenbar $a \in \mathbb{F}_{p^2}$ gelten. Wäre $a \in \mathbb{F}_p$, dann würde $\mathbb{F}_p(a) = \mathbb{F}_p \subsetneq \mathbb{F}_{p^2}$ folgen. Also ist a in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$ enthalten. Zusammen mit dem Ergebnis aus Teil (a) folgt, dass die Elemente $a \in \mathbb{F}_{p^2}$ mit $\mathbb{F}_p(a) = \mathbb{F}_{p^2}$ genau die Elemente der Menge $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$ sind. Die Anzahl der Elemente in dieser Menge ist gegeben durch $|\mathbb{F}_{p^2} \setminus \mathbb{F}_p| = |\mathbb{F}_{p^2}| - |\mathbb{F}_p| = p^2 - p$.

zu (c) Zunächst beweisen wir für alle $a \in \mathbb{F}_{p^6}$ die Äquivalenz

$$\mathbb{F}_p(a) = \mathbb{F}_{p^6} \quad \Leftrightarrow \quad a \notin \mathbb{F}_{p^2} \cup \mathbb{F}_{p^3}.$$

„$\Rightarrow$“ (durch Kontraposition) Ist $a \in \mathbb{F}_{p^2} \cup \mathbb{F}_{p^3}$, dann folgt $a \in \mathbb{F}_{p^2}$ oder $a \in \mathbb{F}_{p^3}$. Im ersten Fall erhalten wir $\mathbb{F}_p(a) \subseteq \mathbb{F}_{p^2} \subsetneq \mathbb{F}_{p^6}$, im zweiten $\mathbb{F}_p(a) \subseteq \mathbb{F}_{p^3} \subsetneq \mathbb{F}_{p^6}$. In beiden Fällen gilt also $\mathbb{F}_p(a) \neq \mathbb{F}_{p^6}$.

„$\Leftarrow$“ Wegen $a \in \mathbb{F}_{p^6}$ ist $\mathbb{F}_p(a)$ ein Zwischenkörper von $\mathbb{F}_{p^6}|\mathbb{F}_p$. Die Zwischenkörper dieser Erweiterung sind gegeben durch $\mathbb{F}_{p^d}$, wobei $d \in \mathbb{N}$ die Teiler von 6 durchläuft, also $d \in \{1, 2, 3, 6\}$ gilt. Im Fall $\mathbb{F}_p(a) = \mathbb{F}_p$ oder $\mathbb{F}_p(a) = \mathbb{F}_{p^2}$ wäre $a \in \mathbb{F}_{p^2}$, im Widerspruch zur Voraussetzung. Im Fall $\mathbb{F}_p(a) = \mathbb{F}_{p^3}$ wäre $a \in \mathbb{F}_{p^3}$, was der Voraussetzung ebenfalls widerspricht. Also muss $\mathbb{F}_p(a) = \mathbb{F}_{p^6}$ gelten.

Aus der soeben bewiesenen Äquivalenz folgt, dass die Anzahl der Elemente $a \in \mathbb{F}_{p^6}$ mit $\mathbb{F}_p(a) = \mathbb{F}_{p^6}$ mit der Anzahl der Elemente in $\mathbb{F}_{p^6} \setminus (\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3})$ übereinstimmt. Zunächst bestimmen wir $|\mathbb{F}_{p^2} \cap \mathbb{F}_{p^3}|$. Es ist $\mathbb{F}_{p^2} \cap \mathbb{F}_{p^3}$ ein gemeinsamer Teilkörper von $\mathbb{F}_{p^2}$ und $\mathbb{F}_{p^3}$, also von der Form $\mathbb{F}_{p^d}$ mit $d \in \mathbb{N}$ und $d \mid 2, 3$. Es folgt $d = 1$ und $\mathbb{F}_{p^2} \cap \mathbb{F}_{p^3} = \mathbb{F}_p$. Damit erhalten wir

$$|\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3}| \quad = \quad |\mathbb{F}_{p^2}| + |\mathbb{F}_{p^3}| - |\mathbb{F}_{p^2} \cap \mathbb{F}_{p^3}| \quad = \quad |\mathbb{F}_{p^2}| + |\mathbb{F}_{p^3}| - |\mathbb{F}_p| \quad = \quad p^2 + p^3 - p.$$

Die gesuchte Elementezahl ist somit $|\mathbb{F}_{p^6} \setminus (\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3})| = |\mathbb{F}_{p^6}| - |\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3}| = p^6 - (p^2 + p^3 - p) = p^6 - p^2 - p^3 + p$.

zu (d) Sei L ein algebraischer Abschluss von $\mathbb{F}_{p^6}$ (und somit zugleich ein algebraischer Abschluss von $\mathbb{F}_p$). Jedes irreduzible, normierte Polynom $f \in \mathbb{F}_p[x]$ vom Grad 6 ist laut Vorlesung separabel, besitzt also laut Vorlesung sechs verschiedene Nullstellen in L. Bezeichnet a eine solche Nullstelle, dann ist f das Minimalpolynom von a über $\mathbb{F}_p$. Daraus folgt $[\mathbb{F}_(a) : \mathbb{F}_p] = \text{grad}(f) = 6$ und somit $\mathbb{F}_p(a) = \mathbb{F}_{p^6}$, denn laut Vorlesung ist $\mathbb{F}_{p^6}|\mathbb{F}_p$ die eindeutig bestimmte Teilerweiterung von $L|\mathbb{F}_p$ vom Grad 6. Wäre

$a \in \mathbb{F}_{p^2} \cup \mathbb{F}_{p^3}$, dann würde $\mathbb{F}_p(a) \subseteq \mathbb{F}_{p^2}$ oder $\mathbb{F}_p(a) \subseteq \mathbb{F}_{p^3}$ und somit $[\mathbb{F}_p(a) : \mathbb{F}_p] \leq [\mathbb{F}_{p^2} : \mathbb{F}_p] = 2$ oder $[\mathbb{F}_p(a) : \mathbb{F}_p] \leq [\mathbb{F}_{p^3} : \mathbb{F}_p] = 3$ folgen, im Widerspruch zu $[\mathbb{F}_p(a) : \mathbb{F}_p] = 6$. Insgesamt haben wir damit gezeigt, dass f genau 6 verschiedene Nullstellen in $\mathbb{F}_{p^6} \setminus (\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3})$ besitzt.

Umgekehrt gilt für jedes $a \in \mathbb{F}_{p^6} \setminus (\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3})$, wie in Teil (c) gezeigt, jeweils $\mathbb{F}_{p^6} = \mathbb{F}_p(a)$. Bezeichnet $f \in \mathbb{F}_p[x]$ das Minimalpolynom von a über $\mathbb{F}_p$, dann folgt $\operatorname{grad}(f) = [\mathbb{F}_p(a) : \mathbb{F}_p] = [\mathbb{F}_{p^6} : \mathbb{F}_p] = 6$. Außerdem ist f normiert, irreduzibel, und es gilt $f(a) = 0$. Also ist jedes $a \in \mathbb{F}_{p^6} \setminus (\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3})$ Nullstelle von einem normierten, irreduziblen Polynom vom Grad 6 in $\mathbb{F}_p[x]$.

Insgesamt ist damit gezeigt, dass die Anzahl der Elemente in $\mathbb{F}_{p^6} \setminus (\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3})$ sechsmal so groß ist wie die Anzahl der normierten, irreduziblen Polynome vom Grad 6. Mit dem Ergebnis von Teil (c) kommen wir zu dem Schluss, dass es genau $\frac{1}{6}(p^6 - p^2 - p^3 + p)$ solche Polynome gibt.

Aufgabe F22T2A5

Betrachten Sie die Teilkörper $K_1 = \mathbb{Q}(\sqrt{3})$ und $K_2 = \mathbb{Q}(\sqrt{6})$ von $\mathbb{C}$.

(a) Zeigen Sie: Für das Kompositum $L = K_1K_2$ gilt $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(b) Beweisen Sie: $K_1 \cap K_2 = \mathbb{Q}$

(c) Bestimmen Sie den Grad der Körpererweiterung $L|\mathbb{Q}$.

(d) Zeigen Sie, dass $L|\mathbb{Q}$ galoissch ist und bestimmen Sie die Galois-Gruppe $\mathrm{Gal}(L|\mathbb{Q})$ bis auf Isomorphie.

(e) Bestimmen Sie sämtliche Zwischenkörper der Erweiterung $L|\mathbb{Q}$.

Lösung:
zu (a) Nach Definition ist das Kompositum gleich $K_1(K_2)$, also die von K_2 erzeugte Erweiterung des Körpers K_1. Zu zeigen ist, dass $K_1(K_2) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ gilt. Für die Inklusion „$\supseteq$“ muss gezeigt werden, dass $\mathbb{Q} \cup \{\sqrt{2}, \sqrt{3}\}$ in $K_1(K_2)$ gezeigt werden, denn daraus folgt, dass $K_1(K_2)$ ein Erweiterungskörper von $\mathbb{Q}$ ist, der $\{\sqrt{2}, \sqrt{3}\}$ enthält, und $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ist nach Definition der kleinste Erweiterungskörper von $\mathbb{Q}$ mit dieser Eigenschaft. Offenbar gilt $\mathbb{Q} \subseteq K_1 \subseteq K_1(K_2)$, und wegen $\sqrt{3} \in K_1$ ist $\sqrt{3}$ auch in $K_1(K_2)$ enthalten. Desweiteren gilt $\sqrt{6} \in K_2$, somit auch $\sqrt{6} \in K_1(K_2)$, und mit $\sqrt{3}$ und $\sqrt{6}$ ist auch $\sqrt{2} = \frac{\sqrt{6}}{\sqrt{3}}$ im Teilkörper $K_1(K_2)$ enthalten.

Für die Inklusion „$\subseteq$“ muss $K_1 \cup K_2 \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ nachgewiesen werden. Wegen $\{\sqrt{3}\} \subseteq \{\sqrt{2}, \sqrt{3}\}$ ist $K_1 = \mathbb{Q}(\sqrt{3})$ in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ enthalten. Für die Inklusion $K_2 = \mathbb{Q}(\sqrt{6}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ genügt es auf Grund der Teilkörper-Eigenschaft von $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ zu zeigen, dass $\mathbb{Q} \cup \{\sqrt{6}\} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ gilt. Die Inklusion $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ ist erfüllt, weil $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ nach Definition ein Erweiterungskörper von $\mathbb{Q}$ ist, und mit $\sqrt{2}$ und $\sqrt{3}$ ist auch das Produkt $\sqrt{6} = \sqrt{2} \cdot \sqrt{3}$ in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ enthalten.

zu (b) Die Inklusion „$\supseteq$“ ist wegen $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) = K_1$ und $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{6}) = K_2$ erfüllt. Für die Inklusion „$\subseteq$“ bemerken wir zunächst, dass $K_1 \cap K_2$ ein Zwischenkörper von $K_1|\mathbb{Q}$ ist. Laut Vorlesung gilt $[\mathbb{Q}(\sqrt{m}) : \mathbb{Q}] = 2$ für jede quadratfreie Zahl $m \in \mathbb{Z} \setminus \{0, 1\}$, insbesondere also $[K_1 : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. Auf Grund der Gradformel gilt

$$2 \quad = \quad [K_1 : \mathbb{Q}] \quad = \quad [K_1 : K_1 \cap K_2] \cdot [K_1 \cap K_2 : \mathbb{Q}] \quad ,$$

daraus folgt $[K_1 \cap K_2 : \mathbb{Q}] \in \{1, 2\}$. Im Fall $[K_1 \cap K_2 : \mathbb{Q}] = 2$ wäre $[K_1 : K_1 \cap K_2] = K_1$ und somit $K_1 = K_1 \cap K_2$, was zu $K_1 \subseteq K_2$ äquivalent ist. Daraus wiederum würde folgen, dass $\sqrt{3}$ in $K_2 = \mathbb{Q}(\sqrt{6})$ enthalten ist. Aus der Vorlesung aber ist bekannt, dass für zwei verschiedene, quadratfreie Zahlen $m, n \in \mathbb{Z}\setminus\{0, 1\}$ jeweils $\sqrt{m} \notin \mathbb{Q}(\sqrt{n})$ gilt. Also muss $[K_1 \cap K_2 : \mathbb{Q}] = 1$ gelten, woraus $K_1 \cap K_2 = \mathbb{Q}$ folgt.

zu (c) Bereits in Teil (b) wurde festgestellt, dass $[K_1 : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ gilt. Das Polynom $f = x^2 - 2 \in \mathbb{Q}(\sqrt{3})[x]$ ist normiert, und es erfüllt $f(\sqrt{2}) = 0$. Wäre es über $\mathbb{Q}(\sqrt{3})$ reduzibel, dann müssten wegen $\mathrm{grad}(f) = 2$ die beiden Nullstellen $\pm\sqrt{2}$ in $\mathbb{Q}(\sqrt{3})$ liegen. Weil aber 2 und 3 zwei verschiedene, quadratfreie Zahlen in $\mathbb{Z} \setminus \{0, 1\}$ sind, gilt $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$. Also ist f in $\mathbb{Q}(\sqrt{3})[x]$ irreduzibel, insgesamt das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}(\sqrt{3})$. Daraus folgt

$$[L : \mathbb{Q}(\sqrt{3})] \quad = \quad [\mathbb{Q}(\sqrt{3})(\sqrt{2}) : \mathbb{Q}(\sqrt{3})] \quad = \quad \mathrm{grad}(f) = 2$$

und $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$.

zu (d) Wir zeigen, dass L ein Zerfällungskörper des Polynoms $g = (x^2 - 2)(x^2 - 3)$ über $\mathbb{Q}$ ist. Daraus folgt, dass $L|\mathbb{Q}$ eine normale und insbesondere eine algebraische Erweiterung ist. Zu zeigen ist $\mathbb{Q}(N) = L$, also $\mathbb{Q}(N) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, wobei N die Menge der komplexen Nullstellen von g bezeichnet. Diese Menge ist gegeben durch $N = \{\pm\sqrt{2}, \pm\sqrt{3}\}$, es ist also $\mathbb{Q}(\{\pm\sqrt{2}, \pm\sqrt{3}\}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ nachzuweisen. Die Inklusion „$\supseteq$“ ist wegen $\{\sqrt{2}, \sqrt{3}\} \subseteq N$ erfüllt. Mit $\sqrt{2}$ und $\sqrt{3}$ sind auch $-\sqrt{2}, -\sqrt{3}$ im Teilkörper $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ von $\mathbb{R}$ enthalten. Somit ist auch die Inklusion „$\subseteq$“ gültig.

Als algebraische Erweiterung von $\mathbb{Q}$ ist $L|\mathbb{Q}$ wegen $\mathrm{char}(\mathbb{Q}) = 0$ auch separabel, insgesamt eine Galois-Erweiterung. Weil $L|\mathbb{Q}$ eine Galois-Erweiterung ist, ist die Ordnung der Galoisgruppe $G = \mathrm{Gal}(L|\mathbb{Q})$ durch $|G| = [L : \mathbb{Q}] = 4$ gegeben. Als Gruppe von Primzahlquadratordnung ist G abelsch, und als endliche abelsche Gruppe ist G isomorph zu einem äußeren direkten Produkt zyklischer Gruppen. Damit gilt entweder $G \cong \mathbb{Z}/4\mathbb{Z}$ oder $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Wäre G zyklisch, also $G \cong \mathbb{Z}/4\mathbb{Z}$, dann gäbe es in G zu jedem Teiler der Gruppenordnung genau eine Untergruppe der entsprechenden Ordnung, insbesondere genau eine Untergruppe U der Ordnung 2, die in G zugleich vom Index 2 ist, wegen $(G : U) = \frac{|G|}{|U|} = \frac{4}{2} = 2$. Daraus wiederum folgt laut Galoistheorie, dass es genau einen Zwischenkörper M von $L|\mathbb{Q}$ mit $[M : \mathbb{Q}] = 2$ gibt.

Nach Teil (a) sind die Elemente $\sqrt{2}, \sqrt{3}, \sqrt{6}$ in L enthalten. Daraus folgt, dass $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ und $\mathbb{Q}(\sqrt{6})$ Zwischenkörper von $L|\mathbb{Q}$ sind. Da es sich bei 2, 3 und 6 um verschiedene quadratfreie Zahlen in $\mathbb{Z} \setminus \{0, 1\}$ handelt, sind diese Zwischenkörper alle vom Grad 2 über $\mathbb{Q}$ und voneinander verschieden. Es gibt also mehr als einen Zwischenkörper von $L|\mathbb{Q}$ vom Grad 2 über $\mathbb{Q}$. Also ist G nicht isomorph zu $\mathbb{Z}/4\mathbb{Z}$, sondern zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

zu (e) Nach dem Hauptsatz der Galoistheorie stimmt die Anzahl der Zwischenkörper von $L|\mathbb{Q}$ mit der Anzahl der Untergruppen von $G = \mathrm{Gal}(L|\mathbb{Q})$ überein, wegen der Isomorphie also auch mit der Anzahl der Untergruppen von $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Nach dem Satz von Lagrange ist die Ordnung jeder Untergruppe ein Teiler von $|\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}| = 4$, also gleich 1, 2 oder 4. Die einzige Untergruppe der Ordnung 1 ist $\{(\bar{0}, \bar{0})\}$, und die einzige Untergruppe der Ordnung 4 ist $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Jede Untergruppe der Ordnung 2 ist zyklisch, wird also von einem Element der Ordnung 2 erzeugt. Daraus folgt, dass $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ genau drei Untergruppen der Ordnung 2 besitzt, nämlich $\langle(\bar{1}, \bar{0})\rangle$, $\langle(\bar{0}, \bar{1})\rangle$ und $\langle(\bar{1}, \bar{1})\rangle$. Insgesamt haben $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ und G also genau fünf Untergruppen, und dementsprechend hat die Erweiterung $L|\mathbb{Q}$ genau fünf Zwischenkörper.

Wie bereits in Teil (d) festgestellt wurde, gibt es drei verschiedene Zwischenkörper vom Grad 2 über $\mathbb{Q}$, nämlich $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ und $\mathbb{Q}(\sqrt{6})$. Hinzu kommen der Zwischenkörper $\mathbb{Q}$ mit $[\mathbb{Q} : \mathbb{Q}] = 1$ und der Zwischenkörper L mit $[L : \mathbb{Q}] = 4$. Damit haben wir alle fünf Zwischenkörper von $L|\mathbb{Q}$ bestimmt.

Aufgabe F22T3A1

Gegeben sei die Gruppe $G = \mathrm{GL}_2(\mathbb{F}_2)$ der invertierbaren 2×2-Matrizen mit Einträgen im Körper $\mathbb{F}_2$.

(a) Listen Sie alle Elemente von G auf.

(b) Zeigen Sie, dass die natürliche Operation von G auf dem Vektorraum $\mathbb{F}_2^2$ einen Isomorphismus $\varphi : G \to \mathrm{Bij}(\mathbb{F}_2^2 \setminus \{0\})$ induziert. (Hierbei bezeichne $\mathrm{Bij}(M)$ die Gruppe der Bijektionen auf einer Mengen M.) Zeigen Sie insbesondere, dass G isomorph ist zu S_3, der symmetrischen Gruppe über 3 Elementen.

(c) Zeigen Sie, dass eine Gruppe der Ordnung 30 höchstens 6 Untergruppen der Ordnung 5 haben kann.

Lösung:
zu (a) Eine 2×2-Matrix über $\mathbb{F}_2$ ist genau dann invertierbar, liegt also in G, wenn die beiden Spaltenvektoren v und w linear unabhängig sind. Die Ordnung von G ist also gleich der Anzahl der Paare (v, w) mit linear unabhängigen $v, w \in \mathbb{F}_2^2$. Für v kann jeder Vektor aus $\mathbb{F}_2^2 \setminus \{(\bar{0}, \bar{0}\}$ gewählt werden; hierfür gibt es genau drei Möglichkeiten. Ist v bereits gewählt, so ist (v, w) genau dann linear unabhängig, wenn $w \in \mathbb{F}_2^2 \setminus \mathrm{lin}(v)$ gilt. Da $\mathrm{lin}(v)$ aus zwei Elementen besteht (nämlich v und dem Nullvektor), stehen für w jeweils $2^2 - 2 = 2$ Elemente zur Auswahl. Insgesamt ist damit gezeigt, dass die Ordnung von G gleich $2 \cdot 3 = 6$ ist. Offenbar sind die sechs Matrizen in der Menge

$$\left\{ \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{1} \end{pmatrix} \right\}$$

alle invertierbar, denn die Determinante jeder Matrix ist gleich $\bar{1}$. Also enthält diese Menge genau die Elemente der Gruppe G.

zu (b) Die natürliche Operation von G auf $\mathbb{F}_2^2$ ist gegeben durch $G \times \mathbb{F}_2^2 \to \mathbb{F}_2^2$, $(A, v) \mapsto Av$. Setzen wir $X = \mathbb{F}_2^2 \setminus \{0\}$, dann erhalten wir durch Einschränkung eine Abbildung $\cdot : G \times X \to \mathbb{F}_2^2$. Für alle $A \in G$ und $v \in X$ ist $Av \neq 0_{\mathbb{F}_2^2}$, also $Av \in X$, denn auf Grund der Invertierbarkeit von A besteht der Kern der linearen Abbildung $\mathbb{F}_2^2 \to \mathbb{F}_2^2$, $v \mapsto Av$ nur aus dem Nullvektor. Also kann $\cdot$ als Abbildung $G \times X \to X$ betrachtet werden.

Wir zeigen, dass durch diese Abbildung eine Gruppenoperation definiert ist. Für alle $v \in X$ und alle $A, B \in G$ gilt $E \cdot v = Ev = v$ und $A \cdot (B \cdot v) = A \cdot (Bv) = A(Bv) = (AB)v = (AB) \cdot v$, wobei E die 2×2-Einheitsmatrix über $\mathbb{F}_2$, also das Neutralelement von G, bezeichnet.

Also ist $\cdot$ tatsächlich eine Gruppenoperation von G auf X. Laut Vorlesung existiert somit ein Gruppenhomomorphismus $\phi : G \to \mathrm{Bij}(X)$ mit $\phi(A)(v) = A \cdot v = Av$ für alle $v \in X$. Zu zeigen ist, dass es sich bei ϕ um einen Isomorphismus handelt. Ist $A \in \ker(\phi)$, dann gilt $Ae_1 = \phi(A)(e_1) = \mathrm{id}_X(e_1) = e_1$. Die erste Spalte von A ist also der erste Einheitsvektor e_1. Genauso zeigt man, dass die zweite Spalte von A gleich e_2 ist. Insgesamt gilt also $A = E$. Damit ist nachgewiesen, dass ϕ injektiv ist. Aus $|X| = |\mathbb{F}_2^2 \setminus \{0_{\mathbb{F}_2^2}\}| = 2^2 - 1 = 3$ folgt außerdem $\mathrm{Bij}(X) \cong S_3$ und somit $|\mathrm{Bij}(X)| = |S_3| = 3! = 6 = |G|$. Als injektive Abbildung zwischen gleichmächtigen endlichen Mengen ist ϕ auch surjektiv, insgesamt ein Isomorphismus. Also ist G isomorph zu $\mathrm{Bij}(X)$, und damit auch zu S_3.

zu (c) Sei G eine Gruppe der Ordnung $30 = 2 \cdot 3 \cdot 5$, und sei ν_5 die Anzahl der 5-Sylowgruppen von G. Auf Grund des Dritten Sylowsatzes gilt $\nu_5 \mid 6$. Es kann also in G höchstens sechs 5-Sylowgruppen geben. Wegen $5^1 \mid 30$, $5^2 \nmid 30$ sind die 5-Sylowgruppen von G genau die Untergruppen der Ordnung 5.

Aufgabe F22T3A2

(a) Bestimmen Sie $a, b \in \mathbb{Z}$ so, dass $(1 + 2\mathbb{Z}) \cap (2 + 3\mathbb{Z}) \cap (3 + 5\mathbb{Z}) = a + b\mathbb{Z}$.

(b) Bestimmen Sie sämtliche ganzzahligen Lösungen $(x, y) \in \mathbb{Z}^2$ der Gleichung $221x + 39y = 26$.

(c) Sei $n \geq 2$ und nehmen wir an, dass $p = 2^n + 1$ eine Primzahl ist. Zeigen Sie, dass eine Restklasse $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ genau dann die Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ erzeugt, wenn a kein Quadrat in $\mathbb{Z}/p\mathbb{Z}$ ist.

Lösung:
zu (a) Eine Zahl $z \in \mathbb{Z}$ liegt genau dann in $(1 + 2\mathbb{Z}) \cap (2 + 3\mathbb{Z}) \cap (3 + 5\mathbb{Z})$, wenn sie die Kongruenzen $z \equiv 1 \bmod 2$, $z \equiv 2 \bmod 3$ und $z \equiv 3 \bmod 5$ erfüllt. Wegen $23 \equiv 1 \bmod 2$, $23 \equiv 2 \bmod 3$ und $23 \equiv 3 \bmod 5$ (und weil Kongruenzrelationen Äquivalenzrelationen, also insbesondere transitiv, sind), ist dies äquivalent zu $z \equiv 23 \bmod n$ für $n \in \{2, 3, 5\}$, also zu $n \mid (z - 23)$ für $n \in \{2, 3, 5\}$. Wegen $\mathrm{kgV}(2, 3, 5) = 30$ ist dies äquivalent zu $30 \mid (z - 23)$, also zu $z \equiv 23 \bmod 30$ und somit zu $z \in 23 + 30\mathbb{Z}$. Die Zahlen $a = 23$ und $b = 30$ haben also die gewünschte Eigenschaft.

zu (b) Für alle $(x, y) \in \mathbb{Z}^2$ ist die Gleichung $221x + 39y = 26$ äquivalent zu $17x + 3y = 2$. Dies wiederum ist äquivalent zu $(17x \equiv 2 \bmod 3) \wedge (y = \frac{1}{3}(2 - 17x))$. Die Kongruenz ist äquivalent zur Gleichung $(2 + 3\mathbb{Z})(x + 2\mathbb{Z}) = 2 + 3\mathbb{Z}$ in $\mathbb{Z}/3\mathbb{Z}$, somit auch zu $x + 2\mathbb{Z} = 1 + 3\mathbb{Z}$, auf Grund der Invertierbarkeit von $2 + 3\mathbb{Z}$ in diesem Ring. Dies wiederum ist äquivalent zur Aussage, dass $x = 1 + 3z$ für ein $z \in \mathbb{Z}$ gilt. Die Menge der ganzzahligen Lösungen der Gleichung ist also gegeben durch $\{(1 + 3z, \frac{1}{3}(2 - 17(1 + 3z))) \mid z \in \mathbb{Z}\}$, was zu $\{(1 + 3z, -5 - 17z) \mid z \in Z\}$ vereinfacht werden kann.

zu (c) Da p eine Primzahl ist, handelt es sich bei $\mathbb{Z}/p\mathbb{Z}$ um einen Körper, und deshalb gilt $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$. Somit gilt $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1 = 2^n$. Laut Vorlesung ist die multiplikative Gruppe eines endlichen Körpers zyklisch, es existiert also ein $c \in (\mathbb{Z}/p\mathbb{Z})^\times$ mit $(\mathbb{Z}/p\mathbb{Z})^\times = \langle c \rangle$. Sei $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ beliebig vorgegeben. Dann existiert ein $j \in \{0, ..., p - 2\}$ mit $a = c^j$.

„$\Leftarrow$“ Ist a kein Quadrat in $\mathbb{Z}/p\mathbb{Z}$, dann muss j ungerade sein, denn wäre j gerade, $j = 2k$ für ein $k \in \mathbb{N}_0$, dann würde $a = c^{2k} = (c^k)^2$ folgen im Widerspruch zur Voraussetzung, dass a kein Quadrat ist. Als ungerade Zahl ist j teilerfremd zur Gruppenordnung 2^n. Daraus folgt laut Vorlesung, dass c und $a = c^j$ dieselbe Ordnung haben. Es gilt also $\mathrm{ord}(a) = 2^n = |(\mathbb{Z}/p\mathbb{Z})^\times|$, und daraus folgt $\langle a \rangle = (\mathbb{Z}/p\mathbb{Z})^\times$.

„$\Rightarrow$“ Wenn a ein Quadrat ist, $a = b^2$ für ein $b \in \mathbb{Z}/p\mathbb{Z}$, dann ist mit a auch b ungleich $\bar{0}$, also eine Einheit. Weil 2 ein Teiler der Gruppenordnung 2^n ist, gilt $\mathrm{ord}(a) = \mathrm{ord}(b^2) \leq \frac{1}{2}\mathrm{ord}(b) = \frac{1}{2}|(\mathbb{Z}/p\mathbb{Z})^\times|$. Wegen $\mathrm{ord}(a) < |(\mathbb{Z}/p\mathbb{Z})^\times|$ kann a kein Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^\times$ sein.

Aufgabe F22T3A3

Es sei $R = \mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ der Ring der ganzen Gauß'schen Zahlen.

(a) Bestimmen Sie die Einheitengruppe von R. Führen Sie einen expliziten und vollständigen Beweis der Korrektheit Ihres Ergebnisses.

(b) Zeigen Sie, dass zwei Elemente $w, z \in R$ genau dann assoziiert sind, wenn $w^4 = z^4$ gilt.

(c) Es sei $(1-i)$ das von dem Element $1-i$ erzeugte Ideal von R. Bestimmen Sie das Ideal $(1-i) \cap \mathbb{Z}$.

Lösung:
zu (a) Sei $N : \mathbb{C} \to \mathbb{R}_+$ die Normfunktion gegeben durch $N(z) = z\bar{z} = |z|^2$ für alle $z \in \mathbb{C}$. Diese Funktion ist multiplikativ, denn für alle $z, w \in \mathbb{C}$ gilt $N(zw) = |zw|^2 = (|z||w|)^2 = |z|^2|w|^2 = N(z)N(w)$. Die Einschränkung von N auf $\mathbb{Z}[i]$ nimmt nur Werte in $\mathbb{N}_0$ an, denn für alle $a, b \in \mathbb{Z}$ gilt $N(a + ib) = |a + ib|^2 = a^2 + b^2 \in \mathbb{N}_0$. Ist nun $\varepsilon = a + ib$ eine Einheit in $\mathbb{Z}[i]$, mit $a, b \in \mathbb{Z}$, dann gilt $N(\varepsilon)N(\varepsilon^{-1}) = N(\varepsilon\varepsilon^{-1}) = N(1) = 1$, und wegen $N(\varepsilon), N(\varepsilon^{-1}) \in \mathbb{N}_0$ folgt daraus $a^2 + b^2 = N(\varepsilon) = 1$. Die Lösungsmenge der Gleichung $a^2 + b^2 = 1$ in $\mathbb{Z}^2$ ist $L = \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$. Aus $(a, b) \in L$ wiederum folgt $\varepsilon = a + ib \in \{1, -1, i, -i\}$. Damit ist $\mathbb{Z}[i]^\times \subseteq \{\pm 1, \pm i\}$ nachgewiesen. Andererseits zeigen die Gleichungen $1 \cdot 1 = (-1) \cdot (-1) = i \cdot (-i) = 1$, dass alle vier Elemente der Menge $\{\pm 1, \pm i\}$ Einheiten sind. Also ist die Einheitengruppe von $\mathbb{Z}[i]$ durch $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ gegeben.

zu (b) Sind $z, w \in \mathbb{Z}[i]$ zueinander assoziiert, dann existiert ein $\varepsilon \in \mathbb{Z}[i]^\times$ mit $w = \varepsilon z$. Nach Teil (a) ist ε damit in der Menge $\{\pm 1, \pm i\}$ enthalten, und wegen $1^4 = (-1)^4 = i^4 = (-i)^4 = 1$ folgt $\varepsilon^4 = 1$. Damit wiederum erhalten wir $w^4 = \varepsilon^4 z^4 = 1 \cdot z^4 = z^4$. Setzen wir umgekehrt $w^4 = z^4$ voraus, dann gilt entweder $w = z = 0$ oder $w, z \neq 0$. Im ersten Fall sind w und z wegen $0 = 1 \cdot 0$ zueinander assoziiert. Ansonsten kann die Gleichung $z^4 = w^4$ zu $(\frac{w}{z})^4 - 1 = 0$ umgeformt werden. Die einzigen komplexen Nullstellen des Polynoms $x^4 - 1$ sind $\pm 1, \pm i$, also die Einheiten von $\mathbb{Z}[i]$. Dies zeigt, dass $w = \frac{w}{z} \cdot z = \varepsilon z$ für ein $\varepsilon \in \mathbb{Z}[i]^\times$ erfüllt, die Elemente w, z also zueinander assoziiert sind.

zu (c) Wir zeigen, dass $(1 - i) \cap Z = 2\mathbb{Z}$ gilt. Als Urbild des Ideals $(1 - i)$ unter dem Inklusionshomomorphismus $\mathbb{Z} \to \mathbb{Z}[i]$, $a \mapsto a$ ist $(1 - i)$ ein Ideal in $\mathbb{Z}$, und dieses enthält 2 wegen $2 \in \mathbb{Z}$ und $2 = (1 + i)(1 - i) \in (1 - i)$. Aus $2 \in (1 - i) \cap Z$ und der Idealeigenschaft von $(1 - i) \cap \mathbb{Z}$ folgt $2\mathbb{Z} \subseteq (1 - i) \cap Z$. Sei nun umgekehrt $a \in (1 - i) \cap \mathbb{Z}$ vorgegeben. Dann gilt $a = \gamma \cdot (1 - i)$ für ein $\gamma \in \mathbb{Z}[i]$. Wegen $a^2 = N(a) = N(\gamma)N(1 - i) = 2N(\gamma)$ ist a^2 gerade. Damit ist auch a gerade, also $a \in 2\mathbb{Z}$.

Aufgabe F22T3A4

Es sei K ein Teilkörper von $\mathbb{C}$, so dass $K|\mathbb{Q}$ eine Galois-Erweiterung vom Grad 4 mit zyklischer Galoisgruppe $\mathrm{Gal}(K|\mathbb{Q})$ ist. Zeigen Sie, dass dann $i \notin K$ gilt.
Hinweis: Nehmen Sie an, dass $i \in K$ gilt und betrachten Sie $K|\mathbb{Q}(i)$.

Lösung:
Sei $G = \mathrm{Gal}(K|\mathbb{Q})$, und nehmen wir an, es gilt $i \in K$. Dann ist $\mathbb{Q}(i)$ ein Zwischenkörper von $K|\mathbb{Q}$. Weil -1 eine quadratfreie Zahl in $\mathbb{Z} \setminus \{0, 1\}$ ist, ist $\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$ eine Erweiterung von $\mathbb{Q}$ vom Grad 2. Laut Galoistheorie ist $U = \mathrm{Gal}(K|\mathbb{Q}(i))$ damit eine Untergruppe vom Index 2, und wegen $|U| = \frac{|G|}{(G:U)} = \frac{4}{2} = 2$ ist diese auch von Ordnung 2. Weil G zyklisch ist, gibt es für jeden Teiler der Gruppenordnung 4 genau eine Untergruppe der Ordnung 4. Daraus folgt, dass U die einzige Untergruppe der Ordnung 2 in G ist.

Sei nun $\rho : K \to \mathbb{C}$ die Einschränkung der komplexen Konjugation $z \mapsto \bar{z}$ auf K. Diese Abbildung ist ein $\mathbb{Q}$-Homomorphismus, und weil $K|\mathbb{Q}$ als Galois-Erweiterung insbesondere normal ist, sogar ein $\mathbb{Q}$-Automorphismus von K, also ein Element der Galoisgruppe G. Für alle $\alpha \in K$ gilt $\rho^2(\alpha) = \rho(\bar{\alpha}) = \bar{\bar{\alpha}} = \alpha$, also $\rho^2 = \mathrm{id}_K$. Wegen $i \in K$ und $\rho(i) = -i \neq i$ ist andererseits $\rho \neq \mathrm{id}_K$. Also ist $\rho \in G$ ein Element der Ordnung 2. Weil U die einzige Untergruppe der Ordnung 2 in G ist, muss $\langle \rho \rangle = U$ und insbesondere $\rho \in U$ gelten. Aber wegen $U = \mathrm{Gal}(K|\mathbb{Q}(i))$ folgt daraus $\rho(i) = i$, im Widerspruch zu $\rho(i) = -i$. Also ist die Annahme $i \in K$ falsch, und es folgt $i \notin K$.

Aufgabe F22T3A5

Es sei $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)$.

(a) Bestimmen Sie den Grad der Körpererweiterung $K|\mathbb{Q}$.

(b) Entscheiden und begründen Sie, ob es einen $\mathbb{Q}$-Homomorphismus $\varphi : K \to \mathbb{C}$ mit $\varphi(\sqrt[3]{2}) = \sqrt{3}$ gibt.

(c) Entscheiden und begründen Sie, ob die Erweiterung $K|\mathbb{Q}$ galoissch ist.

Lösung:

zu (a) Das Polynom $f = x^3 - 2 \in \mathbb{Q}[x]$ ist irreduzibel auf Grund des Eisenstein-Kriteriums (angewendet auf die Primzahl 2), es ist normiert und erfüllt $f(\sqrt[3]{2}) = 0$. Also ist f das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$, und wir erhalten $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \operatorname{grad}(f) = 3$. Weil 3 eine quadratfreie Zahl in $\mathbb{Z} \setminus \{0, 1\}$ ist, gilt laut Vorlesung $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. Das Polynom $g = x^2 - 3 \in \mathbb{Q}(\sqrt[3]{2})[x]$ ist normiert und erfüllt $g(\sqrt{3}) = 0$. Wäre es in $\mathbb{Q}(\sqrt[3]{2})[x]$ reduzibel, dann müsste die Nullstelle $\sqrt{3}$ von g wegen $\operatorname{grad}(g) = 2$ in $\mathbb{Q}(\sqrt[3]{2})$ liegen. Es wäre dann $\mathbb{Q}(\sqrt{3})$ ein Zwischenkörper von $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$, und die Gradformel würde

$$3 \quad = \quad [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(\sqrt{3})] \cdot 2$$

liefern. Es gilt aber $2 \nmid 3$, und somit ist g in $\mathbb{Q}(\sqrt[3]{2})[x]$ irreduzibel. Somit ist g das Minimalpolynom von $\sqrt{3}$ über $\mathbb{Q}(\sqrt[3]{2})$, und es folgt $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}(\sqrt[3]{2})] = \operatorname{grad}(g) = 2$. Schließlich ist das Polynom $h = x^2 + 1 \in \mathbb{Q}(\sqrt[3]{2}, \sqrt{3})[x]$ normiert und erfüllt $h(i) = 0$. Wäre es über $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$ reduzibel, dann müsste wegen $\operatorname{grad}(h) = 2$ die Nullstelle i in $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$ liegen. Aber dies ist wegen $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) \subseteq \mathbb{R}$ und $i \notin \mathbb{R}$ nicht der Fall. Also ist h in $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})[x]$ irreduzibel, insgesamt das Minimalpolynom von h über $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$. Daraus folgt

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i) : \mathbb{Q}(\sqrt[3]{2}, \sqrt{3})] \quad = \quad \operatorname{grad}(h) \quad = \quad 2.$$

Mit der Gradformel erhalten wir nun

$$\begin{aligned}[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i) : \mathbb{Q}] \quad &= \quad [[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i) : [\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})] \cdot [\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \\ &= \quad 2 \cdot 2 \cdot 3 \quad = \quad 12.\end{aligned}$$

zu (b) Nehmen wir an, ein $\mathbb{Q}$-Homomorphismus φ wie angegeben existiert. Ist $f \in \mathbb{Q}[x]$ und $\alpha \in \mathbb{C}$ eine Nullstelle von f, dann muss laut Vorlesung $\varphi(\alpha)$ eine Nullstelle desselben Polynoms sein. Da nun $\sqrt[3]{2}$ eine Nullstelle von $f = x^3 - 2$ ist, müsste auch $\varphi(\sqrt[3]{2}) = \sqrt{3}$ eine Nullstelle von f sein. Tatsächlich gilt aber $f(\sqrt{3}) \neq 0$, denn die komplexen Nullstellen von f sind $\sqrt[3]{2}$, $\zeta\sqrt[3]{2}$ und $\zeta^2\sqrt[3]{2}$ mit $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$, insbesondere ist $\sqrt[3]{2}$ die einzige reelle Nullstelle. Also existiert kein $\mathbb{Q}$-Homomorphismus $\varphi : K \to \mathbb{C}$ mit $\varphi(\sqrt[3]{2}) = \sqrt{3}$.

Anmerkung:

In der Orginalfassung der Aufgabenstellung war von einem $\mathbb{Q}$-Automorphismus $K \to \mathbb{C}$ die Rede. Das ist natürlich nicht sinnvoll, denn bei einem Automorphismus (egal ob von Körpern, Ringen, Gruppen oder Vektorräumen) müssen Definitions- und Wertebereich stets übereinstimmen.

zu (c) Wir zeigen, dass die Erweiterung $K|\mathbb{Q}$ normal ist, indem wir nachweisen, dass es sich bei K um den Zerfällungskörper des Polynoms $g = (x^3 - 2)(x^2 + 1) \in \mathbb{Q}[x]$ über $\mathbb{Q}$ handelt. Wie bereits in Teil (b) festgestellt, ist $\{\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}\}$ mit $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ die Menge der komplexen Nullstellen von $x^3 - 2$, und $\pm i$ sind die komplexen Nullstellen von $x^2 + 1$. Daraus folgt, dass $N = \{\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}, i, -i\}$ die Nullstellenmenge von g ist. Zu zeigen ist also

$$\mathbb{Q}(N) \quad = \quad \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i).$$

„$\subseteq$“ Es genügt, $N \subseteq \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)$ nachzuweisen. mit $\sqrt{3}$ und i ist auch $\sqrt{-3} = i\sqrt{3}$ in $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)$ enthalten, damit auch $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ und ζ^2. Da auch $\sqrt[3]{2}$ und $\pm i$ in $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)$ liegen, folgt insgesamt $N = \{\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}, i, -i\} \subseteq \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)$.

„$\supseteq$“ Zu zeigen ist $\{\sqrt[3]{2}, \sqrt{3}, i\} \subseteq \mathbb{Q}(N)$. Wegen $\sqrt[3]{2}, i \in N$ gilt $\sqrt[3]{2}, i \in \mathbb{Q}(N)$. Mit $\sqrt[3]{2} \in \mathbb{Q}(N)$ und $\zeta\sqrt[3]{2} \in \mathbb{Q}(N)$ gilt auch $\zeta = \frac{\zeta\sqrt[3]{2}}{\sqrt[3]{2}} \in \mathbb{Q}(N)$ und damit auch $\sqrt{-3} = 2\zeta + 1 \in \mathbb{Q}(N)$. Aus $\sqrt{-3} \in \mathbb{Q}(N)$ und $i \in N \subseteq \mathbb{Q}(N)$ folgt $\sqrt{3} = (-i)\sqrt{-3} \in \mathbb{Q}(N)$. Damit ist die Inklusion $\{\sqrt[3]{2}, \sqrt{3}, i\} \subseteq \mathbb{Q}(N)$ vollständig nachgewiesen.

Als normale Erweiterung ist $K|\mathbb{Q}$ insbesondere algebraisch, und wegen $\mathrm{char}(\mathbb{Q}) = 0$ damit auch separabel. Insgesamt ist $K|\mathbb{Q}$ also tatsächlich eine Galois-Erweiterung.

Aufgabe H22T1A1

Gegeben sei die Gruppe

$$G \quad = \quad \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathcal{M}_{2,\mathbb{Q}} \;\middle|\; a, b, c \in \mathbb{Q}, ac \neq 0 \right\}$$

der invertierbaren oberen 2×2-Dreiecksmatrizen über $\mathbb{Q}$. Ferner seien

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G \;\middle|\; c = a \right\} \qquad \text{und} \qquad U = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G \;\middle|\; b = 0 \right\}.$$

(a) Zeigen Sie, dass H ein Normalteiler von G ist und dass durch

$$\varphi : G/H \to \mathbb{Q}^\times \quad \text{mit} \quad \varphi\left(\left[\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right] \right) = \frac{a}{c}$$

ein wohldefinierter Gruppenisomorphismus gegeben ist.

(b) Zeigen Sie, dass U eine Untergruppe von G, aber kein Normalteiler ist.

(c) Betrachten Sie die Operation von U auf H durch Konjugation. Geben Sie ein Repräsentantensystem der Bahnen dieser Gruppenoperation an.

Lösung:

zu (a) Wir beweisen die Existenz des angegebenen Isomorphismus durch Anwendung des Homomorphiesatzes für Gruppen. Sei $\hat{\varphi} : G \to \mathbb{Q}^\times$ gegeben durch

$$\hat{\varphi}\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right) \quad = \quad \frac{a}{c} \qquad \text{für} \quad a, c \in \mathbb{Q}^\times \text{ und } b \in \mathbb{Q}.$$

Diese Abbildung ist ein Gruppenhomomorphismus, denn für alle $a, a_1, c, c_1 \in \mathbb{Q}^\times$ und alle $b, b_1 \in \mathbb{Q}$ gilt

$$\hat{\varphi}\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \right) \quad = \quad \hat{\varphi}\left(\begin{pmatrix} aa_1 & ab_1 + bc_1 \\ 0 & cc_1 \end{pmatrix} \right) \quad = \quad \frac{aa_1}{cc_1}(aa_1)(cc_1) \quad = \quad \frac{a}{c} \cdot \frac{a_1}{c_1}$$

$$= \quad \hat{\varphi}\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right) \hat{\varphi}\left(\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \right).$$

Für alle $a, c \in \mathbb{Q}^\times$ und $b \in \mathbb{Q}$ gilt die Äquivalenz

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \ker(\hat{\varphi}) \quad \Leftrightarrow \quad \hat{\varphi}\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right) = 1 \quad \Leftrightarrow \quad \frac{a}{c} = 1 \quad \Leftrightarrow \quad c = a \quad \Leftrightarrow \quad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in H.$$

Dies zeigt, dass $H = \ker(\hat{\varphi})$ gilt. Als Kern eines Gruppenhomomorphismus $G \to \mathbb{Q}^\times$ ist H ein Normalteiler von G. Darüber hinaus ist $\hat{\varphi}$ surjektiv. Ist nämlich $a \in \mathbb{Q}^\times$ vorgegeben, dann gilt

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in G \text{ wegen } a \cdot 1 = a \neq 0 \quad \text{und außerdem} \quad \hat{\varphi}\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \right) = a \cdot 1 = a.$$

Damit ist nachgewiesen, dass $\hat{\varphi}$ die Voraussetzungen des Homomorphiesatzes erfüllt. Auf Grund des Satzes existiert ein wohldefinierter Isomorphismus $G/H \to \mathbb{Q}^\times$ gegeben durch

$$\left[\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right] \quad \mapsto \quad \hat{\varphi}\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right) = ac$$

für alle $a, c \in \mathbb{Q}^\times$ und $b \in \mathbb{Q}$. Dieser stimmt offenbar mit der in der Aufgabenstellung angegebenen Abbildung überein.

zu (b) Zunächst zeigen wir, dass U eine Untergruppe von G ist. Das Neutralelement von G ist die Einheitsmatrix E_2, und diese ist offenbar in U enthalten (setze $a = c = 1$. Seien nun $A, A_1 \in U$ vorgegeben. Dann sind auch AA_1 und A^{-1} in U enthalten. Denn wegen $A, A_1 \in U$ gibt es $a, a_1, c, c_1 \in \mathbb{Q}^\times$ mit

$$A = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \quad \text{und} \quad A_1 = \begin{pmatrix} a_1 & 0 \\ 0 & c_1 \end{pmatrix} \quad ,$$

und es folgt

$$AA_1 = \begin{pmatrix} aa_1 & 0 \\ 0 & cc_1 \end{pmatrix} \in U \quad \text{und} \quad A^{-1} \begin{pmatrix} a^{-1} & 0 \\ 0 & c^{-1} \end{pmatrix} \in U$$

wegen $aa_1, cc_1 \in \mathbb{Q}^\times$. Wäre U ein Normalteiler, dann wäre wegen

$$B = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in U \quad \text{und} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in G$$

auch TBT^{-1} in U enthalten. Tatsächlich aber gilt

$$\begin{aligned} TBT^{-1} &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & -2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix} \notin U. \end{aligned}$$

zu (c) Um zu erkennen, welche Gestalt die Bahnen der Gruppenoperation haben, wenden wir ein beliebiges Element der Gruppe U auf ein beliebiges Element der Menge H an. Für alle $a, a_1, c \in \mathbb{Q}^\times$ und $b_1 \in \mathbb{Q}$ gilt

$$\begin{aligned} \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} &= \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}^{-1} = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & c^{-1} \end{pmatrix} \\ &= \begin{pmatrix} aa_1 & ab_1 \\ 0 & ca_1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & c^{-1} \end{pmatrix} = \begin{pmatrix} a_1 & ab_1c^{-1} \\ 0 & a_1 \end{pmatrix}. \end{aligned}$$

Ist $b_1 = 0$, dann besteht die Bahn also nur aus der Diagonalmatrix a_1E_2, ansonsten durchläuft der Eintrag rechts oben alle Elemente aus $\mathbb{Q}^\times$. Dies führt uns zu der Behauptung, dass die Teilmenge $R \subseteq H$ gegeben durch

$$R = \left\{ \begin{pmatrix} a_1 & \varepsilon_1 \\ 0 & a_1 \end{pmatrix} \;\middle|\; a_1 \in \mathbb{Q}^\times \;,\; \varepsilon_1 \in \{0, 1\} \right\}$$

ein Repräsentantensystem der Bahnen der Operation ist. Bezeichnet $\mathcal{B}$ die Menge der Bahnen, so müssen wir nachweisen, dass die Abbildung $\phi : R \to \mathcal{B}$, $A \mapsto U(A)$ surjektiv und injektiv ist. Zum Nachweis der Surjektivität sei $U(A) \in \mathcal{B}$ vorgegeben, mit

$$A = \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} \in H \quad , \quad a_1 \in \mathbb{Q}^\times,\ b_1 \in \mathbb{Q}.$$

Ist $b_1 = 0$, dann liegt A selbst bereits in R, und es gilt $\phi(A) = U(A)$. Betrachten wir nun den Fall $b_1 \neq 0$. Dann gilt

$$\begin{pmatrix} a_1 & 1 \\ 0 & a_1 \end{pmatrix} \in R \quad \text{und} \quad \begin{pmatrix} 1 & 0 \\ 0 & b_1 \end{pmatrix} \in U$$

wegen $a_1 \in \mathbb{Q}^\times$ und $1, b_1 \in \mathbb{Q}^\times$, und außerdem

$$\begin{pmatrix} 1 & 0 \\ 0 & b_1 \end{pmatrix} \cdot \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & b_1 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & b_1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & b_1 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & b_1^{-1} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & b_1 \end{pmatrix} \begin{pmatrix} aa_1 & 1 \\ 0 & a_1 b_1^{-1} \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ 0 & a_1 \end{pmatrix}.$$

Es folgt

$$\begin{pmatrix} a_1 & 1 \\ 0 & a_1 \end{pmatrix} \in U\left(\begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix}\right)$$

und somit

$$\phi\left(\begin{pmatrix} a_1 & 1 \\ 0 & a_1 \end{pmatrix}\right) = U\left(\begin{pmatrix} a_1 & 1 \\ 0 & a_1 \end{pmatrix}\right) = U\left(\begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix}\right).$$

Damit ist der Nachweis der Surjektivität abgeschlossen.

Zum Nachweis der Injektivität seien

$$\begin{pmatrix} a & \varepsilon \\ 0 & a \end{pmatrix}, \begin{pmatrix} a_1 & \varepsilon_1 \\ 0 & a_1 \end{pmatrix} \in R \quad \text{mit} \quad \phi\left(\begin{pmatrix} a & \varepsilon \\ 0 & a \end{pmatrix}\right) = \phi\left(\begin{pmatrix} a_1 & \varepsilon_1 \\ 0 & a_1 \end{pmatrix}\right)$$

vorgegeben, wobei $a, a_1 \in \mathbb{Q}^\times$ und $\varepsilon, \varepsilon_1 \in \{0, 1\}$ sind. Nach Definition der Abbildung ϕ folgt

$$U\left(\begin{pmatrix} a & \varepsilon \\ 0 & a \end{pmatrix}\right) = U\left(\begin{pmatrix} a_1 & \varepsilon_1 \\ 0 & a_1 \end{pmatrix}\right) \quad \text{und} \quad \begin{pmatrix} a_1 & \varepsilon_1 \\ 0 & a_1 \end{pmatrix} \in U\left(\begin{pmatrix} a & \varepsilon \\ 0 & a \end{pmatrix}\right).$$

Es gibt also ein Element

$$\begin{pmatrix} a_2 & 0 \\ 0 & c_2 \end{pmatrix} \in U \quad \text{mit} \quad \begin{pmatrix} a_1 & \varepsilon_1 \\ 0 & a_1 \end{pmatrix} = \begin{pmatrix} a_2 & 0 \\ 0 & c_2 \end{pmatrix} \cdot \begin{pmatrix} a & \varepsilon \\ 0 & a \end{pmatrix}$$

und $a_2, c_2 \in \mathbb{Q}^\times$. Es gilt also

$$\begin{pmatrix} a_1 & \varepsilon_1 \\ 0 & a_1 \end{pmatrix} = \begin{pmatrix} a_2 & 0 \\ 0 & c_2 \end{pmatrix} \cdot \begin{pmatrix} a & \varepsilon \\ 0 & a \end{pmatrix} = \begin{pmatrix} a_2 & 0 \\ 0 & c_2 \end{pmatrix} \begin{pmatrix} a & \varepsilon \\ 0 & a \end{pmatrix} \begin{pmatrix} a_2 & 0 \\ 0 & c_2 \end{pmatrix}^{-1} =$$

$$\begin{pmatrix} a_2 & 0 \\ 0 & c_2 \end{pmatrix} \begin{pmatrix} a & \varepsilon \\ 0 & a \end{pmatrix} \begin{pmatrix} a_2^{-1} & 0 \\ 0 & c_2^{-1} \end{pmatrix} = \begin{pmatrix} a_2 & 0 \\ 0 & c_2 \end{pmatrix} \begin{pmatrix} aa_2^{-1} & \varepsilon c_2^{-1} \\ 0 & ac_2^{-1} \end{pmatrix} = \begin{pmatrix} a & a_2 \varepsilon c_2^{-1} \\ 0 & a \end{pmatrix}$$

Durch Vergleich der Einträge erhalten wir $a_1 = a$ und $\varepsilon_1 = a_2 \varepsilon c_2^{-1}$. Wieder unterscheiden wir zwei Fälle. Ist $\varepsilon = 0$, dann folgt $\varepsilon_1 = 0$ und somit insgesamt

$$\begin{pmatrix} a & \varepsilon \\ 0 & a \end{pmatrix} = \begin{pmatrix} a_1 & \varepsilon_1 \\ 0 & a_1 \end{pmatrix}.$$

Ist $\varepsilon = 1$, dann folgt $\varepsilon_1 = a_2 \varepsilon c_2^{-1} \neq 0$, wegen $\varepsilon_1 \in \{0, 1\}$ also $\varepsilon_1 = 1$. Dies zeigt, dass die beiden Elemente aus R auch in diesem Fall übereinstimmen.

Aufgabe H22T1A2

Sei R der Faktorring $\mathbb{Q}[x]/(x^2-7x+12)$.

(a) Zeigen Sie, dass R als Ring isomorph zu $\mathbb{Q}\times\mathbb{Q}$ ist.

(b) Geben Sie explizit einen Ringisomorphismus $\varphi:\mathbb{Q}\times\mathbb{Q}\to R$ an.

(c) Bestimmen Sie alle Zahlen $a\in\mathbb{Q}$, so dass die Restklasse von $x+a$ in R eine Einheit ist, und finden Sie jeweils das dazu inverse Element.

Lösung:
zu (a) Die p-q-Formel liefert für das Polynom $f=x^2-7x+12$ die Nullstellen 3 und 4. Die Polynome $x-3$ und $x-4$ sind als Polynome vom Grad 1 irreduzibel, und da sie nicht zueinander assoziiert sind, sind sie teilerfremd. Der Chinesische Restsatz kann somit angewendet werden und liefert einen Isomorphismus

$$\bar{\phi}: R=\mathbb{Q}[x]/(f)\to\mathbb{Q}[x]/(x-3)\times\mathbb{Q}[x]/(x-4)\quad,\quad g+(f)\mapsto(g+(x-3),g+(x-4))$$

von Ringen. Für jedes $a\in\mathbb{Q}$ sei $\rho_a:\mathbb{Q}[x]\to g$, $g\mapsto g(a)$ der Auswertungshomomorphismus an der Stelle a. Dieser ist surjektiv, denn für vorgegebenes $c\in\mathbb{Q}$ gilt $\rho_a(c)=c(a)=c$. Es gilt $\ker(\rho_a)=(x-a)$, auf Grund der Äquivalenz

$$g\in\ker(\rho_a)\quad\Leftrightarrow\quad\rho_a(g)=0\quad\Leftrightarrow\quad g(a)=0\quad\Leftrightarrow\quad(x-a)\mid g\quad\Leftrightarrow\quad g\in(x-a)$$

für alle $g\in\mathbb{Q}[x]$. Der Homomorphiesatz für Ringe ist also anwendbar und liefert für jedes $a\in\mathbb{Q}$ einen Isomorphismus $\bar{\rho}_a:\mathbb{Q}[x]/(x-a)\to\mathbb{Q}$, $g+(x-a)\mapsto g(a)$. Durch $(g+(x-3),g+(x-4))\mapsto(g(3),g(4))$ ist somit ein Isomorphismus $\psi:\mathbb{Q}[x]/(x-3)\times\mathbb{Q}[x]/(x-4)\to\mathbb{Q}\times\mathbb{Q}$ definiert, und insgesamt ist $\bar{\phi}\circ\psi$ ein Isomorphismus zwischen R und $\mathbb{Q}\times\mathbb{Q}$.

zu (b) Die Gleichung $1\cdot(x-3)+(-1)\cdot(x-4)=1$ kann zu $1+(3-x)=4-x$ umgestellt werden und liefert wegen $\bar{\phi}(4-x+(f))=((4-x)+(x-3),(4-x)+(x-4))=(1+(x-3),0+(x-4))$ ein Urbild von $(1+(x-3),0+(x-4))\in\mathbb{Q}[x]/(x-3)\times\mathbb{Q}[x]/(x-4)$ bezüglich $\bar{\phi}$. Ebenso überprüft man, dass der Isomorphismus $\bar{\phi}$ das Element $x-3+(f)$ auf $(0+(x-3),1+(x-4))$ abbildet. Für alle $h_1,h_2\in\mathbb{Q}[x]$ gilt

$$\begin{aligned}\bar{\phi}((4-x)h_1+(x-3)h_2+(f)) &= \bar{\phi}(h_1+(f))\bar{\phi}(4-x+(f))+\bar{\phi}(h_2+(f))\bar{\phi}(x-3+(f))\\ &= (h_1+(x-3),h_1+(x-4))(1+(x-3),0+(x-4))+\\ &\quad(h_2+(x-3),h_2+(x-4))(0+(x-3),1+(x-4)) =\\ &\quad(h_1+(x-3),0+(x-4))+(0+(x-3),h_2+(x-4)) = (h_1+(x-3),h_2+(x-4)).\end{aligned}$$

Dies zeigt, dass die Umkehrabbildung von $\bar{\phi}$ durch $\bar{\phi}^{-1}(h_1+(x-3),h_2+(x-4))=(4-x)h_1+(x-3)h_2+(f)$ gegeben ist. Die Umkehrabbildung von ψ ist offenbar gegeben durch $\psi^{-1}(c,d)=(c+(x-3),d+(x-4))$ für alle $(c,d)\in\mathbb{Q}\times\mathbb{Q}$, denn es gilt jeweils $\psi(c+(x-3),d+(x-4))=(c(3),d(4))=(c,d)$. Die Abbildung $\bar{\phi}^{-1}\circ\psi^{-1}$ ist ein Isomorphismus $\mathbb{Q}\times\mathbb{Q}\to\mathbb{Q}[x]/(f)$, und dieser ist explizit gegeben durch

$$\begin{aligned}(\bar{\phi}^{-1}\circ\psi^{-1})(c,d) &= \bar{\phi}^{-1}(c+(x-3),d+(x-4)) = c(4-x)+d(x-3)+(f)\\ &= (d-c)x+4c-3d+(f)\end{aligned}$$

für alle $c,d\in\mathbb{Q}$.

zu (c) Sei $a \in \mathbb{Q}$. Da es sich bei $\psi \circ \bar{\phi}$ um einen Isomorphismus von Ringen handelt, ist das Element $x-a+(f)$ genau dann eine Einheit in R, wenn $(\psi \circ \bar{\phi})(x-a+(f)) = \psi(x-a+(x-3), x-a+(x-4)) = (3-a, 4-a)$ eine Einheit in $\mathbb{Q}$ ist. Wegen $(\mathbb{Q} \times \mathbb{Q})^\times = \mathbb{Q}^\times \times \mathbb{Q}^\times = (\mathbb{Q} \setminus \{0\}) \times (\mathbb{Q} \setminus \{0\})$ ist dies genau dann der Fall, wenn $3-a \neq 0$ und $4-a \neq 0$ gilt, also genau dann, wenn $a \notin \{3, 4\}$ gilt.

Das Inverse von $(\psi \circ \bar{\phi})(x-a+(f)) = (3-a, 4-a)$ in $\mathbb{Q} \times \mathbb{Q}$ ist $(\frac{1}{3-a}, \frac{1}{4-a})$. Das Inverse von $x-a+(f)$ in R ist somit gegeben durch

$$\begin{aligned}(\psi \circ \bar{\phi})^{-1}(\tfrac{1}{3-a}, \tfrac{1}{4-a}) &= (\bar{\phi}^{-1} \circ \psi^{-1})(\tfrac{1}{3-a}, \tfrac{1}{4-a}) = \bar{\phi}^{-1}\left(\tfrac{1}{3-a} + (x-3), \tfrac{1}{4-a} + (x-4)\right) \\ &= \frac{4-x}{3-a} + \frac{x-3}{4-a} + (f).\end{aligned}$$

Anmerkung:
Dass dieses Element tatsächlich das Inverse von $x-a+(f)$ ist, kann auch durch eine direkte Rechnung überprüft werden: Wegen $(4-a)(3-a) = f(a)$ gilt

$$\begin{aligned}\left(\frac{4-x}{3-a} + \frac{x-3}{4-a} + (f)\right) \cdot (x-a+(f)) &= \left(\frac{(4-x)(4-a)+(x-3)(3-a)}{f(a)} + (f)\right) \cdot (x-a+(f)) \\ &= \big(f(a)^{-1}((16-4x-4a+ax)+(3x-9-ax+3a)) + (f)\big) \cdot (x-a+(f)) \\ = \big(f(a)^{-1}(-x+7-a)+(f)\big) \cdot (x-a+(f)) &= f(a)^{-1}(-x+7-a)(x-a)+(f) \\ = f(a)^{-1}(-x^2+7x+a(a-7))+(f) &= f(a)^{-1}(-x^2+7x+a(a-7)+f)+(f)) \\ = f(a)^{-1}(-x^2+7x+a(a-7)+x^2-7x+12)+(f) &= f(a)^{-1}(a(a-7)+12)+(f) \\ = f(a)^{-1}(a^2-7a+12)+(f) = f(a)^{-1}f(a)+(f) &= 1+(f) = 1_R.\end{aligned}$$

Aufgabe H22T1A3

(a) Sei $L|K$ eine endliche Galois-Erweiterung und sei $a \in L$. Zeigen Sie, dass a genau dann ein primitives Element für $L|K$ ist, wenn die Elemente $\sigma(a)$ für alle $\sigma \in \mathrm{Gal}(L|K)$ paarweise verschieden sind.

(b) Beweisen Sie, dass $\mathbb{Q}(\sqrt{3}, i)|\mathbb{Q}$ eine Galois-Erweiterung ist und bestimmen Sie die Elemente der Galois-Gruppe.

(c) Zeigen Sie, dass für alle $q \in \mathbb{Q} \setminus \{0\}$ das Element $a = \sqrt{3} + qi$ ein primitives Element der Galois-Erweiterung $\mathbb{Q}(\sqrt{3}, i)|\mathbb{Q}$ ist.

Lösung:
zu (a) „⇒“ Nach Voraussetzung gilt $L = K(a)$. Daraus folgt, dass jedes Element $\sigma \in \mathrm{Gal}(L|K)$ durch das Bild $\sigma(a)$ bereits eindeutig bestimmt ist. Sind also $\sigma, \tau \in \mathrm{Gal}(L|K)$ mit $\sigma(a) = \tau(a)$, dann folgt $\sigma = \tau$. Setzen wir umgekehrt $\sigma \neq \tau$ voraus, dann muss also $\sigma(a) \neq \tau(a)$ gelten.

„⇐“ Auf Grund der Voraussetzung folgt für jedes $\sigma \in \mathrm{Gal}(L|K)$ aus $\sigma(a) = a = \mathrm{id}_L(a)$ bereits $\sigma = \mathrm{id}_L$. Ist nun $\sigma \in \mathrm{Gal}(L|K(a))$, dann gilt $\sigma(\gamma) = \gamma$ für alle $\gamma \in K(a)$, insbesondere also $\sigma(a) = a$ und somit $\sigma = \mathrm{id}_L$. Es gilt also $\mathrm{Gal}(L|K(a)) = \{\mathrm{id}_L\} = \mathrm{Gal}(L|L)$. Nach dem Hauptsatz der Galoistheorie ist $M \mapsto \mathrm{Gal}(L|M)$ eine bijektive Korrespondenz zwischen den Zwischenkörpern von $L|K$ und den Untergruppen von $\mathrm{Gal}(L|K)$. Aus der Gleichheit $\mathrm{Gal}(L|K(a)) = \mathrm{Gal}(L|L)$ folgt also $L = K(a)$, d.h. a ist ein primitives Element der Erweiterung $L|K$.

zu (b) Die Elemente $\sqrt{3}$ und i sind Nullstellen des Polynoms $f = (x^2 - 3)(x^2 + 1) \in \mathbb{Q}[x]$ und somit algebraisch über $\mathbb{Q}$. Daraus folgt, dass $\mathbb{Q}(\sqrt{3}, i)|\mathbb{Q}$ eine algebraische Körpererweiterung ist. Wegen $\mathrm{char}(\mathbb{Q}) = 0$ ist $\mathbb{Q}(\sqrt{3}, i)|\mathbb{Q}$ als algebraische Erweiterung auch separabel. Darüber hinaus ist die Erweiterung normal. Um dies zu zeigen, weisen wir nach, dass $\mathbb{Q}(\sqrt{3}, i)$ in $\mathbb{C}$ der Zerfällungskörper von f über $\mathbb{Q}$ ist. Offenbar sind die Elemente der Menge $N = \{\pm\sqrt{3}, \pm i\}$ Nullstellen von f, und wegen $\mathrm{grad}(f) = 4 = |N|$ kann es keine weiteren geben. Somit ist $\mathbb{Q}(N)$ der Zerfällungskörper von f über $\mathbb{Q}$. Wegen $\sqrt{3}, i \in N$ gilt $\mathbb{Q}(\sqrt{3}, i) \subseteq \mathbb{Q}(N)$. Umgekehrt enthält $\mathbb{Q}(\sqrt{3}, i)$ neben $\sqrt{3}$ und i auch $-\sqrt{3}$ und $-i$ (weil $\mathbb{Q}(\sqrt{3}, i)$ als Teilkörper von $\mathbb{C}$ abgeschlossen unter der Bildung von Negativen ist). Es gilt also $N \subseteq \mathbb{Q}(\sqrt{3}, i)$, und weil $\mathbb{Q}(\sqrt{3}, i)$ ein Zwischenkörper von $\mathbb{C}|\mathbb{Q}$ ist, folgt daraus auch $\mathbb{Q}(N) \subseteq \mathbb{Q}(\sqrt{3}, i)$, insgesamt also $\mathbb{Q}(N) = \mathbb{Q}(\sqrt{3}, i)$.

Also handelt es sich bei $\mathbb{Q}(\sqrt{3}, i)|\mathbb{Q}$ tatsächlich um eine Galois-Erweiterung. Sei G die zugehörige Galois-Gruppe; laut Vorlesung ist die Ordnung dieser Gruppe durch $|G| = [\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}]$ gegeben. Laut Vorlesung gilt $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$, weil 3 eine quadratfreie ganze Zahl ungleich $0, 1$ ist. Das Polynom $g = x^2 + 1$ ist normiert und hat i als Nullstelle. Wäre es über $\mathbb{Q}(\sqrt{3})$ reduzibel, dann wären wegen $\mathrm{grad}(g)$ die beiden Nullstellen $\pm i$ in $\mathbb{Q}(\sqrt{3})$ enthalten. Aber dies ist unmöglich, denn wegen $\sqrt{3} \in \mathbb{R}$ gilt einerseits $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}$, andererseits aber $\pm i \in \mathbb{C} \setminus \mathbb{R}$. Also ist g über $\mathbb{Q}(\sqrt{3})$ irreduzibel, insgesamt das Minimalpolynom von i über $\mathbb{Q}(\sqrt{3})$. Es folgt

$$[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}(\sqrt{3})] \quad = \quad [\mathbb{Q}(\sqrt{3})(i) : \mathbb{Q}(\sqrt{3})] \quad = \quad \mathrm{grad}(g) \quad = \quad 2 \quad ,$$

und mit der Gradformel erhalten wir $|G| = [\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$.

Weil das Polynom g über $\mathbb{Q}(\sqrt{3})$ irreduzibel ist, und weil $\pm i$ Nullstellen von g sind, existiert auf Grund des Fortsetzungssatzes ein Element $\tau \in \mathrm{Gal}(\mathbb{Q}(\sqrt{3}, i)|\mathbb{Q}(\sqrt{3}))$ mit $\tau(i) = -i$. Insbesondere ist τ ein Element der Gruppe G, mit $\tau(\sqrt{3}) = \sqrt{3}$ und $\tau(i) = -i$. Das Polynom $h = x^2 - 3$ ist irreduzibel über $\mathbb{Q}(i)$. Wäre es nämlich reduzibel, dann würden die beiden Nullstellen $\pm\sqrt{3}$ bereits in $\mathbb{Q}(i)$ liegen, und daraus würde $\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(i)$ folgen. Da -1 eine quadratfreie Zahl in $\mathbb{Z} \setminus \{0, 1\}$ ist, ergäbe sich daraus $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = [\mathbb{Q}(i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{-1}) : \mathbb{Q}] = 2$. Aber dies steht Widerspruch zu unserer Feststellung $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = 4$ von oben. Da $\pm\sqrt{3}$ Nullstellen von h sind, liefert der Fortsetzungssatz ein Element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{3}, i)|\mathbb{Q}(i))$ mit $\sigma(\sqrt{3}) = -\sqrt{3}$, also ein Element $\sigma \in G$ mit $\sigma(\sqrt{3}) = -\sqrt{3}$ und $\sigma(i) = i$.

Neben $\mathrm{id}_{\mathbb{Q}(\sqrt{3},i)}$, σ und τ ist $\sigma \circ \tau$ ein weiteres Element der Gruppe G. Dieses stimmt mit keinem der drei anderen Elemente überein, denn es gilt einerseits $(\sigma \circ \tau)(i) = \sigma(-i) = -\sigma(i) = -i$ und somit $\sigma \circ \tau \neq \mathrm{id}_{\mathbb{Q}(\sqrt{3},i)}, \sigma$ (wegen $\mathrm{id}_{\mathbb{Q}(\sqrt{3},i)}(i) = \sigma(i) = i$), andererseits aber auch $(\sigma \circ \tau)(\sqrt{3}) = \sigma(\sqrt{3}) = -\sqrt{3}$ und somit $\sigma \circ \tau \neq \tau$ (wegen $\tau(\sqrt{3}) = \sqrt{3}$). Wegen $|G| = 4$ ist damit insgesamt $G = \{\mathrm{id}_{\mathbb{Q}(\sqrt{3},i)}, \sigma, \tau, \sigma \circ \tau\}$ nachgewiesen.

zu (c) Sei $q \in \mathbb{Q} \setminus \{0\}$ und $a = \sqrt{3} + iq$. Nach Teil (b) sind $\mathrm{id}_{\mathbb{Q}(\sqrt{3},i)}$, σ, τ und $\sigma \circ \tau$ die Elemente von $\mathrm{Gal}(\mathbb{Q}(\sqrt{3}, i)|\mathbb{Q})$, und es gilt $\mathrm{id}_{\mathbb{Q}(\sqrt{3},i)}(a) = \sqrt{3} + iq$, $\sigma(a) = -\sqrt{3} + iq$, $\tau(a) = \sqrt{3} - iq$ und $(\sigma \circ \tau)(a) = \sigma(\sqrt{3} - iq) = -\sqrt{3} - iq$. Je zwei dieser komplexen Zahlen unterscheiden sich im Real- oder Imaginärteil. Die vier Bilder von a unter den Elementen der Galois-Gruppe sind also paarweise verschieden. Nach Teil (a) folgt daraus, dass a ein primitives Element der Erweiterung $\mathbb{Q}(\sqrt{3}, i)|\mathbb{Q}$ ist.

Aufgabe H22T1A4

Betrachten Sie das Polynom $f = x^4 + 5x^2 + 5 \in \mathbb{Q}[x]$. Es sei $Z \subseteq \mathbb{C}$ sein Zerfällungskörper in $\mathbb{C}$ und $\alpha \in Z$ eine Nullstelle.

(a) Dividieren Sie das Polynom f durch $x^2 - \alpha^2 \in \mathbb{Q}(\alpha)[x]$, ohne die Nullstelle exiplizit zu berechnen.

(b) Zeigen Sie, dass die Gleichung $(\alpha^3 + 3\alpha)^2 = -(5 + \alpha^2)$ gilt.

(c) Zeigen Sie, dass $[Z : \mathbb{Q}] = 4$ und $\mathrm{Gal}(Z|\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$ gilt.

Lösung:
zu (a) Entsprechend der Vorgehensweise bei der Polynomdivision berechnen wir zunächst die Differenz $f - x^2(x^2 - \alpha^2) = f - x^4 + \alpha^2 x^2 = (5 + \alpha^2)x^2 + 5$ und subtrahieren anschließend $(5 + \alpha^2)(x^2 - \alpha^2)$. Wir erhalten

$$\begin{aligned}(5 + \alpha^2)x^2 + 5 - (5 + \alpha^2)(x^2 - \alpha^2) &= 5x^2 + \alpha^2 x^2 + 5 - 5x^2 - \alpha^2 x^2 + 5\alpha^2 + \alpha^4 = \\ 5 + 5\alpha^2 + \alpha^4 &= f(\alpha) = 0.\end{aligned}$$

Insgesamt gilt also

$$f - x^2(x^2 - \alpha^2) - (5 + \alpha^2)(x^2 - \alpha^2) = 0$$

was zu $f = (x^2 + \alpha^2 + 5)(x^2 - \alpha^2)$ umgeformt werden kann.

zu (b) Das Polynom $f \in \mathbb{Z}[x]$ ist auf Grund des Eisenstein-Kriteriums (angewendet auf die Primzahl 5) irreduzibel über $\mathbb{Z}$ und damit auch über $\mathbb{Q}$. Außerdem ist es normiert, und es gilt $f(\alpha) = 0$. Insgesamt handelt es sich also um das Minimalpolynom von α über $\mathbb{Q}$. Laut Vorlesung folgt daraus, dass $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \mathrm{grad}(f) = 4$ und $\mathcal{B} = \{1, \alpha, \alpha^2, \alpha^3\}$ eine Basis von $\mathbb{Q}(\alpha)$ als $\mathbb{Q}$-Vektorraum ist. Die Elemente $(\alpha^3 + 3\alpha)^2$ und $-(5 + \alpha)^2$ stimmen also genau dann überein, wenn ihre Darstellung als Linearkombination von $\mathcal{B}$ übereinstimmt.

Nun gilt einerseits $-(5 + \alpha^2) = (-5) + (-1)\alpha^2$. Um auch $(\alpha^3 + 3\alpha)^2$ als Linearkombination von $\mathcal{B}$ darzustellen, formen wir die Gleichung $\alpha^4 + 5\alpha^2 + 5 = f(\alpha) = 0$ zunächst zu $\alpha^4 = -5 - 5\alpha^2$ um. Wir erhalten dann $\alpha^6 = \alpha^2 \cdot \alpha^4 = \alpha^2(-5 - \alpha^2) = -5\alpha^2 - 5\alpha^4 = -5\alpha^2 + 25 + 25\alpha^2 = 20\alpha^2 + 25$. Es folgt

$$(\alpha^3 + 3\alpha)^2 = \alpha^6 + 6\alpha^4 + 9\alpha^2 = 20\alpha^2 + 25 - 30\alpha^2 - 30 + 9\alpha^2 = (-5) + (-1)\alpha^2.$$

Also stimmen die Elemente tatsächlich überein.

zu (c) Bereits in Teil (b) wurde nachgewiesen, dass $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ ist. Nun zeigen wir noch, dass $\mathbb{Q}(\alpha)$ mit dem Zerfällungskörper Z von f über $\mathbb{Q}$ übereinstimmt und erhalten somit die gewünschte Gleichung $[Z : \mathbb{Q}] = 4$. Nach Definition gilt $Z = \mathbb{Q}(N)$, wobei N die Menge der komplexen Nullstellen von f bezeichnet. Zu zeigen ist also $\mathbb{Q}(\alpha) = \mathbb{Q}(N)$. Wegen $f(\alpha) = 0$ gilt $\alpha \in N$ und somit $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(N)$. Für die umgekehrte Inklusion genügt es, $N \subseteq \mathbb{Q}(\alpha)$ zu Überprüfen. Die Zerlegung

$$f = (x^2 + \alpha^2 + 5)(x^2 - \alpha^2)$$

aus Teil (a) zeigt, dass $\pm\alpha$ in N liegen.

Aus der Gleichung $(\alpha^3+3\alpha)^2 = -(5+\alpha^2)$ aus Teil (b) folgt, dass auch $\pm(3\alpha+\alpha^3)$ Nullstellen von f sind, denn es gilt

$$\begin{aligned} f(3\alpha+\alpha^3) &= ((3\alpha+\alpha^3)^2+\alpha^2+5)((3\alpha+\alpha^3)^2-\alpha^2) = \\ (-(5+\alpha^2)+\alpha^2+5)((3\alpha+\alpha^3)^2-\alpha^2) &= 0\cdot((3\alpha+\alpha^3)^2-\alpha^2) = 0 \quad , \end{aligned}$$

und ebenso erhält man $f(-3\alpha-\alpha^3)=0$. Die Elemente $\pm\alpha$ und $\pm(3\alpha+\alpha^3)$ sind paarweise verschieden, denn wie in Teil (b) gezeigt wurde, ist $\mathcal{B}=\{1,\alpha,\alpha^2,\alpha^3\}$ eine vierelementige Basis von $\mathbb{Q}(\alpha)$ als $\mathbb{Q}$-Vektorraum, und für beliebige $b_0,b_1,b_2,b_3\in\mathbb{Q}$ und $c_0,c_1,c_2,c_3\in\mathbb{Q}$ gilt somit

$$b_0+b_1\alpha+b_2\alpha^2+b_3\alpha^3 = c_0+c_1\alpha+c_2\alpha^2+c_3\alpha^3$$

dann und nur dann, wenn $b_j=c_j$ für $0\le j\le 3$ erfüllt ist. Da f als Polynom vom Grad 4 nicht mehr als vier komplexe Nullstellen besitzen kann, muss $N=\{\pm\alpha,\pm(3\alpha+\alpha^3)\}$ gelten. Dies zeigt, dass N tatsächlich in $\mathbb{Q}(\alpha)$ enthalten ist.

Als Zerfällungskörper des Polynoms $f\in\mathbb{Q}[x]$ über $\mathbb{Q}$ ist Z ein normaler Erweiterungskörper von $\mathbb{Q}$. Insbesondere ist die Erweiterung $Z|\mathbb{Q}$ algebraisch, und wegen $\mathrm{char}(\mathbb{Q})=0$ somit auch separabel. Insgesamt handelt es sich bei $Z|\mathbb{Q}$ um eine Galois-Erweiterung, und laut Vorlesung folgt daraus $|\mathrm{Gal}(f|\mathbb{Q})| = \mathrm{Gal}(Z|\mathbb{Q}) = [Z:\mathbb{Q}] = 4$. Für den Isomorphismus $\mathrm{Gal}(f|\mathbb{Q})\cong\mathbb{Z}/4\mathbb{Z}$ genügt es somit zu zeigen, dass in $\mathrm{Gal}(f|\mathbb{Q})$ ein Element der Ordnung 4 existiert. Weil f irreduzibel ist und α und $3\alpha+\alpha^3$ Nullstellen von f sind, existiert auf Grund des Fortsetzungssatzes ein Element $\sigma\in\mathrm{Gal}(f|\mathbb{Q})$ mit $\sigma(\alpha)=3\alpha+\alpha^3$. Wegen $|\mathrm{Gal}(f|\mathbb{Q})|=4$ ist nur $\mathrm{ord}(\sigma)\in\{1,2,4\}$ möglich. Um zu zeigen, dass $\mathrm{ord}(\sigma)=4$ gilt, genügt es somit $\sigma^2\neq\mathrm{id}_Z$ nachzuweisen, und hierfür wiederum ist $\sigma^2(\alpha)\neq\alpha$ hinreichend. Mit Hilfe der Gleichungen $\alpha^4=-5-5\alpha^2$, $\alpha^6=20\alpha^2+25$ und $(3\alpha+\alpha^3)^2=-5-\alpha^2$ aus Teil (b) erhalten wir

$$\begin{aligned} (3\alpha+\alpha^3)^3 &= (3\alpha+\alpha^3)^2(3\alpha+\alpha^3) = (-5-\alpha^2)(3\alpha+\alpha^3) = -15\alpha-3\alpha^3-5\alpha^3-\alpha^5 \\ &= -15\alpha-8\alpha^3-\alpha^4\alpha = -15\alpha-8\alpha^3+(5+5\alpha^2)\alpha \\ &= -15\alpha-8\alpha^3+5\alpha+5\alpha^3 = -10\alpha-3\alpha^3 \end{aligned}$$

und somit

$$\begin{aligned} \sigma^2(\alpha) &= \sigma(\sigma(\alpha)) = \sigma(3\alpha+\alpha^3) = 3\sigma(\alpha)+\sigma(\alpha)^3 = 3(3\alpha+\alpha^3)+(3\alpha+\alpha^3)^3 \\ &= 9\alpha+3\alpha^3-10\alpha-3\alpha^3 = -\alpha. \end{aligned}$$

Also gilt tatsächlich $\sigma^2(\alpha)\neq\alpha$.

Aufgabe H22T1A5

Sei $\Phi_n \in \mathbb{Q}[x]$ das n-te Kreisteilungspolynom über $\mathbb{Q}$. Zeigen Sie:

(a) Es gilt $x^n - 1 = (x-1)h$ mit einem Polynom $h \in \mathbb{Q}[x]$ mit $h(1) = n$.

(b) Ist $n = p^k$ für eine Primzahl p und $k \geq 1$, so gilt $\Phi_n(1) = p$.

(c) Hat n mindestens zwei Primzahlen $p \neq q$ als Teiler, so ist $\Phi_n(1) = 1$.

Lösung:
zu (a) Bekanntlich gilt $x^n - 1 = (x-1)h$ mit $h = \sum_{k=0}^{n-1} x^k$, und es ist $h(1) = \sum_{k=0}^{n-1} 1^k = \sum_{k=0}^{n-1} 1 = n$.

zu (b) Laut Vorlesung ist das Kreisteilungspolynom zu einer Primzahlpotenz p^k (mit $k \geq 1$) gegeben durch $\Phi_{p^k} = \sum_{j=0}^{p-1} x^{jp^{k-1}}$. Folglich gilt $\Phi_{p^k}(1) = \sum_{j=0}^{p-1} 1^{jp^{k-1}} = \sum_{j=0}^{p-1} 1 = p$.

zu (c) Wir beweisen die folgenden beiden Aussagen.

(i) Ist $n \in \mathbb{N}$ und sind p, q zwei verschiedene Primteiler von n, dann gilt $\Phi_n(1) \mid n$, aber $p \nmid \Phi_n(1)$ und $q \nmid \Phi_n(1)$.

(ii) Es gilt $\Phi_n(1) > 0$ für alle $n \in \mathbb{N}$ mit $n \geq 2$.

Aus Teil (i) folgt, dass $\Phi_n(1)$ keine Primteiler hat, sobald n mindestens zwei verschiedene Primteiler besitzt, in diesem Fall also $\Phi_n(1) \in \{\pm 1\}$ gilt. Zusammen mit (ii) folgt dann $\Phi_n(1) = 1$, wie gewünscht.

zu (i) Aus der Vorlesung ist bekannt, dass $x^n - 1 = \prod_{d|n} \Phi_d$ gilt, wobei d die Teiler von n in $\mathbb{N}$ durchläuft. Nach Teil (a) existiert ein Polynom $h_n \in \mathbb{Z}[x]$ mit $x^n - 1 = (x-1)h_n$ und $h_n(1) = n$. Wir erhalten

$$(x-1)h_n \quad = \quad x^n - 1 \quad = \quad (x-1) \prod_{\substack{d \mid n \\ d \neq 1}} \Phi_d \quad ,$$

und die Anwendung der Kürzungsregel im Integritätsbereich $\mathbb{Q}[x]$ liefert $h_n = \prod_{d|n, d\neq 1} \Phi_d = \Phi_n \cdot \prod_{d|n, d\neq 1, n} \Phi_d$. Dies zeigt, dass $\Phi_n(1)$ ein Teiler von $h_n(1) = n$ ist. Seien nun $a, b \in \mathbb{N}$ so gewählt, dass $n = p^a q^b m$ gilt, mit einem zu p und q teilerfremden m, und setzen wir $S = \{d \in \mathbb{N} \mid d \mid n, d \nmid p^a, d \nmid q^b, d \neq n\}$. Dann können wir das Polynom h_n in der Form

$$h_n \quad = \quad \prod_{k=1}^{a} \Phi_{p^k} \cdot \prod_{\ell=1}^{b} \Phi_{q^\ell} \cdot \Phi_n \cdot r$$

mit $r = \prod_{d \in S} \Phi_d \in \mathbb{Z}[x]$ schreiben. Mit Hilfe der Ergebnisse von Teil (a) und (b) erhalten wir

$$p^a q^b m \quad = \quad n \quad = \quad h_n(1) \quad = \quad p^a \cdot q^b \cdot \Phi_n(1) \cdot r(1)$$

und somit $m = \Phi_n(1) \cdot r(1)$. Es folgt $\Phi_n(1) \mid m$. Wegen $\mathrm{ggT}(m, pq) = 1$ ergibt sich daraus wiederum $p \nmid \Phi_n(1)$ und $q \nmid \Phi_n(1)$.

zu (ii) Diese Aussage beweisen wir durch vollständige Induktion über n. Für $n = 2$ ist sie offenbar erfüllt, denn es gilt $\Phi_2 = x + 1$ und $\Phi_2(1) = 1 + 1 = 2 > 0$. Sei nun $n \in \mathbb{N}$ mit $n > 2$, und setzen wir die Aussage für natürliche Zahlen kleiner als n voraus. Wie oben gezeigt, gilt $h_n = \Phi_n \cdot \prod_{d|n, d\neq 1, n} \Phi_d$ und somit auch $h_n(1) = \Phi_n(1) \cdot \prod_{d|n, d\neq 1, n} \Phi_d(1)$. Es ist $h_n(1) = n > 0$, und nach Induktionsvoraussetzung gilt $\Phi_d(1) > 0$ für alle Teiler $d \in \mathbb{N}$ von n mit $d \neq 1, n$. Auf Grund der obigen Gleichung muss somit auch $\Phi_n(1) > 0$ gelten.

Aufgabe H22T2A1

Eine *affine Ebene* in $\mathbb{R}^3$ ist die Menge aller Punkte $(x, y, z) \in \mathbb{R}^3$, die eine Gleichung der Form $ax + by + cz + d = 0$ erfüllen mit fest vorgegebenen Zahlen $a, b, c, d \in \mathbb{R}$ und $(a, b, c) \neq (0, 0, 0)$.

(a) Für $j = 1, 2, 3, 4$ seien vier Punkte $P_j = (x_j, y_j, z_j) \in \mathbb{R}^3$ gegeben. Zeigen Sie, dass P_1, P_2, P_3, P_4 genau dann in einer affinen Ebene liegen, wenn gilt

$$\begin{vmatrix} x_1 & y_1 & z_1 & 1 \\ x_2 & y_2 & z_2 & 1 \\ x_3 & y_3 & z_3 & 1 \\ x_4 & y_4 & z_4 & 1 \end{vmatrix} = 0.$$

(b) Sei $C = \{(t, t^2, t^3) \in \mathbb{R}^3 \mid t \in \mathbb{R}\}$, und sei $E \subseteq \mathbb{R}^3$ eine affine Ebene. Zeigen Sie, dass $C \cap E$ höchstens drei Elemente hat.

Lösung:
zu (a) Seien $a, b, c, d \in \mathbb{R}$ mit $(a, b, c) \neq (0, 0, 0)$. Es liegen P_1, P_2, P_3, P_4 genau dann auf der Ebene

$$E_{a,b,c,d} = \{(x, y, z) \in \mathbb{R}^3 \mid ax + by + cz + d = 0\} ,$$

wenn $ax_j + by_j + cz_j + d = 0$ für $j = 1, 2, 3, 4$ gilt. Die Punkte liegen also genau dann auf einer affinen Ebene, wenn das linearen Gleichungssystem

$$x_j a + y_j b + z_j c + d = 0 \quad (1 \leq j \leq 4)$$

eine Lösung $(a, b, c, d) \in \mathbb{R}^4$ mit $(a, b, c) \neq (0, 0, 0)$ besitzt. Dies ist genau dann der Fall, wenn das lineare Gleichungssystem $Ax = 0_{\mathbb{R}^4}$ mit der Matrix

$$A = \begin{pmatrix} x_1 & y_1 & z_1 & 1 \\ x_2 & y_2 & z_2 & 1 \\ x_3 & y_3 & z_3 & 1 \\ x_4 & y_4 & z_4 & 1 \end{pmatrix}$$

eine Lösung dieser Form besitzt. Wir zeigen, dass dies genau dann der Fall ist, wenn $\det A = 0$ gilt.

„⇒“ Existiert eine Lösung der angegebenen Form, dann ist insbesondere $\ker A \neq \{0_{\mathbb{R}^4}\}$ und $\dim \ker A \geq 1$. Mit dem Dimensionssatz für lineare Abbildungen folgt daraus $4 - \operatorname{rg}(A) \geq 1$, was zu $\operatorname{rg}(A) < 4$ und $\det A = 0$ äquivalent ist. „⇐“ Aus $\det A = 0$ folgt $\operatorname{rg}(A) < 4$, was auf Grund der Dimensionssatzes zu $\dim \ker A \geq 1$ und $\ker A \neq \{0_{\mathbb{R}^4}\}$ äquivalent ist. Sei $(a, b, c, d) \in \mathbb{R}^4$ ein Element des Kerns ungleich null. Wäre $(a, b, c) = (0, 0, 0)$, dann würde wegen

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} x_1 & y_1 & z_1 & 1 \\ x_2 & y_2 & z_2 & 1 \\ x_3 & y_3 & z_3 & 1 \\ x_4 & y_4 & z_4 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ d \end{pmatrix} = \begin{pmatrix} d \\ d \\ d \\ d \end{pmatrix}$$

auch $d = 0$ und somit $(a, b, c, d) = (0, 0, 0, 0)$ folgen, im Widerspruch zur Voraussetzung. Also ist (a, b, c, d) eine Lösung des LGS mit $(a, b, c) \neq (0, 0, 0)$.

zu (b) Sei $p \in \mathbb{R}^3$ und $E = E_{a,b,c}$ eine affine Ebene. Dann gilt die Äquivalenz

$$\begin{aligned} p \in E \cap C \quad &\Leftrightarrow \quad p \in E \text{ und } p \in C \quad \Leftrightarrow \quad p \in E \text{ und } \exists\, t \in \mathbb{R} : p = (t, t^2, t^3) \\ &\Leftrightarrow \quad \exists\, t \in \mathbb{R} : p = (t, t^2, t^3) \text{ und } at + bt^2 + ct^3 + d = 0. \end{aligned}$$

Also gilt $p \in E \cap C$ genau dann, wenn ein $t \in \mathbb{R}$ mit $p = (t, t^2, t^3)$ existiert, das Nullstelle des Polynoms $f_{a,b,c} = cx^3 + bx^2 + ax + d \in \mathbb{R}[x]$ ist. Wegen $(a, b, c) \neq (0, 0, 0)$ ist $f_{a,b,c}$ nicht das Nullpolynom. Da es als Polynom ungleich null vom Grad ≤ 3 höchstens drei Nullstellen besitzt (und jeder Schnittpunkt $p \in \mathbb{R}^3$ durch die zugehörige Nullstelle $t \in \mathbb{R}$ eindeutig festgelegt ist) gibt es höchstens drei Schnittpunkte von E und C.

Aufgabe H22T2A2

Sei K ein Körper, sei $K[x]$ der Polynomring über K in einer Unbestimmten, und sei $L = K(x)$ der Quotientenkörper von $K[x]$. Sei weiter

$$R \quad = \quad \left\{ \frac{a}{b} \;\middle|\; a, b \in K[x] \ , \ \mathrm{ggT}(a,b) = 1 \ , \ b(0) \neq 0 \right\} \quad \subseteq \quad L.$$

Zeigen Sie:

(a) Die Menge R ist ein Teilring von L.

(b) Sei I ein Ideal von R. Dann ist $I \cap K[x]$ ein Ideal von $K[x]$.

(c) Der Ring R ist ein Hauptidealring.

Lösung:
zu (a) Zu überprüfen ist, dass $1_{K(x)} \in R$ gilt, und dass mit $u, v \in R$ auch $u - v$ und uv in R liegen. Da K ein Teilring von $K[x]$ und $K[x]$ ein Teilring von $K(x)$ ist, ist K ein Teilring von $K(x)$. Sei $a = b = 1_K$. Dann gilt $a, b \in K[x]$ und $b(0_K) = 1_K \neq 0_K$, außerdem $\mathrm{ggT}(a,b) = \mathrm{ggT}(1_K, 1_K) = 1_K$. Insgesamt erhalten wir $1_{K(x)} = 1_K = \frac{1_K}{1_K} \in R$.

Seien $u, v \in R$. Dann gibt es $a_1, a_2, b_1, b_2 \in K[x]$ mit $u = \frac{a_1}{b_1}$, $v = \frac{a_2}{b_2}$ und $b_1(0_K) \neq 0_K$, $b_2(0_K) \neq 0_K$. Es folgt

$$uv \quad = \quad \frac{a_1 a_2}{b_1 b_2} \quad \text{mit} \quad a_1 a_2, b_1 b_2 \in K[x] \quad \text{und} \quad (b_1 b_2)(0_K) = b_1(0_K) b_2(0_K) \neq 0 \quad ,$$

da $b_1(0_K), b_2(0_K) \neq 0_K$ und K ein Körper ist. Sei nun $d \in R$ ein größter gemeinsamer Teiler von $a_1 a_2$ und $b_1 b_2$. Dann gibt es teilerfremde $a_3, b_3 \in K[x]$ mit $a_1 a_2 = d a_3$ und $b_1 b_2 = d b_3$. Es folgt

$$uv \quad = \quad \frac{a_1 a_2}{b_1 b_2} \quad = \quad \frac{d a_3}{d b_3} \quad = \quad \frac{a_3}{b_3}$$

und außerdem $b_3(0_K) \neq 0$, da ansonsten $(b_1 b_2)(0_K) = d(0_K) b_3(0_K)$ gleich 0_K wäre. Insgesamt ist damit $uv \in R$ nachgewiesen. Ebenso gilt

$$u - v \quad = \quad \frac{a_1}{b_1} - \frac{a_2}{b_2} \quad = \quad \frac{a_1 b_2 - a_2 b_1}{b_1 b_2}$$

mit $a_1 b_2 - a_2 b_1 \in K[x]$, $b_1 b_2 \in K[x]$ und $(b_1 b_2)(0_K) \neq 0_K$. Sei $d' \in R$ ein größter gemeinsamer Teiler von $a_1 b_2 - a2 b_1$ und $b_1 b_2$. Dann gibt es teilerfremde $a_4, b_4 \in K[x]$ mit $a_1 b_2 - a2 b_1 = d' a_4$ und $b_1 b_2 = d' b_4$. Es folgt

$$u - v \quad = \quad \frac{a_1 b_2 - a_2 b_1}{b_1 b_2} \quad = \quad \frac{d' a_4}{d' b_4} \quad = \quad \frac{a_4}{b_4}.$$

Dabei ist $b_4(0_K) \neq 0$, da ansonsten $(b_1 b_2)(0_K) = d'(0_K) b_4(0_K)$ gleich 0_K wäre. Insgesamt zeigt dies, dass auch $u - v$ in R liegt.

zu (b) Sei I ein Ideal in R. Zu zeigen ist, dass $I \cap K[x]$ ein Ideal in $K[x]$ ist. Wir betrachten dazu die Abbildung $\phi : K[x] \to K(x)$, $f \mapsto \frac{f}{1_K}$. Für jedes $f \in K[x]$ gilt $\mathrm{ggT}(f, 1_K) = 1_K$ und $1_K(0_K) = 1_K \neq 0_K$, also $f = \frac{f}{1} \in R$. Dies zeigt, dass ϕ als Abbildung $K[x] \to R$ aufgefasst werden kann. Diese Abbildung ist ein Ringhomomorphismus, denn es gilt $\phi(1_{K[x]}) = \phi(1_K) = \frac{1_K}{1_K} = 1_R$ und für alle $f, g \in K[x]$ außerdem

$$\phi(f+g) \quad = \quad \frac{f+g}{1_K} \quad = \quad \frac{f}{1_K} + \frac{g}{1_K} \quad = \quad \phi(f) + \phi(g)$$

und

$$\phi(fg) \quad = \quad \frac{fg}{1_K} \quad = \quad \frac{f}{1_K} \cdot \frac{g}{1_K} \quad = \quad \phi(f)\phi(g).$$

Es ist $I \cap K[x] = \phi^{-1}(I)$, denn für alle $f \in K[x]$ gilt die Äquivalenz

$$f \in \phi^{-1}(I) \quad = \quad \phi(f) \in I \quad = \quad \frac{f}{1_K} \in I \quad = \quad f \in I \quad = \quad f \in I \cap K[x].$$

Als Urbild eines Ideals in R unter einem Ringhomomorphismus $K[x] \to R$ ist $I \cap K[x]$ ein Ideal in $K[x]$.

zu (c) Wir müssen überprüfen, dass R ein Integritätsbereich und jedes Ideal in R ein Hauptideal ist. Ersteres ist der Fall, weil R nach Teil (a) Teilring eines Körpers, nämlich $K(x)$, ist. Für den Nachweis der zweiten Aussage sei I ein Ideal in R. Nach Teil (b) ist $I \cap K[x]$ ein Ideal in $K[x]$. Da es sich bei $K[x]$ (als Polynomring über einem Körper) um einen Hauptidealring handelt, existiert ein $f \in K[x]$ mit $I \cap K[x] = fK[x]$. (Wir verwenden die Notation $fK[x]$ an Stelle der üblichen Schreibweise (f) für das von f erzeugte Ideal, um deutlich zu machen, dass hier das Erzeugnis von f im Ring $K[x]$ gemeint ist.) Wir zeigen nun, dass auch I ein Hauptideal ist, indem wir die Gleichung

$$I \quad = \quad fR \qquad \text{überprüfen.}$$

„$\supseteq$“ Es gilt $f \in K[x] \cap I$, damit insbesondere $f \in I$. Weil I ein Ideal in R ist, folgt daraus $fR \subseteq I$. „$\subseteq$“ Sei $u \in I$ vorgegeben. Dann liegt u insbesondere in R, es gibt also $a, b \in K[x]$ mit $u = \frac{a}{b}$, $b(0_K) \neq 0_K$ und $\mathrm{ggT}(a, b) = 1_K$. Das Element $bu = a$ ist dann in $K[x] \cap I$ enthalten. Wegen $K[x] \cap I = fK[x]$ existiert ein $r \in K[x]$ mit $bu = a = rf$. Sei $d \in K[x]$ ein größter gemeinsamer Teiler von b und r. Dann gibt es teilerfremde Elemente $b_1, r_1 \in K[x]$ mit $b = db_1$ und $r = dr_1$, und es folgt $db_1u = dr_1f$. Weil $K[x]$ ein Integritätsbereich ist, dann die Kürzungsregel angewendet werden, und wir erhalten $b_1u = r_1f$. Es folgt $u = f\frac{r_1}{b_1}$, wegen $\frac{r_1}{b_1} \in R$ also $u \in fR$.

Aufgabe H22T2A3

(a) Es ist $337 = 2\cdot 3\cdot 5\cdot 11+7 = 13\cdot 17+2^2\cdot 29$. Erklären Sie, dass daraus folgt, dass 337 eine Primzahl ist.

(b) Sei p eine Primzahl und $n \geq 1$. Zeigen Sie, dass die Gleichung $x^n = \bar{1}$ in $\mathbb{F}_p$ genau $\mathrm{ggT}(n, p-1)$ verschiedene Lösungen besitzt.

(c) Ermitteln Sie alle positiven ganzen Zahlen n, für die die Gleichung $x^n = 1$ im Ring $\mathbb{Z}/2022\mathbb{Z}$ genau n Lösungen hat.

Lösung:

zu (a) Wäre 337 keine Primzahl, dann gäbe es einen Primteiler p von 337 mit $p \leq \sqrt{337}$. Wegen $\sqrt{337} < 19$ ist 17 die größte Primzahl $\leq \sqrt{337}$. Es genügt deshalb zu zeigen, dass 337 keinen Primteiler ≤ 17 besitzt, mit anderen Worten, die Zahlen 2, 3, 5, 7, 11, 13 und 17 müssen als Teiler von 337 ausgeschlossen werden. Wäre eine der Zahlen $2, 3, 5$ oder 11 ein Teiler von 337, dann müsste diese Zahl auf Grund der Gleichung $337 = 2\cdot 3\cdot 5\cdot 11+7$ auch ein Teiler von 7 sein, was aber unmöglich ist, da es sich um eine von 7 verschiedene Primzahl handelt. Ebenso zeigt die Gleichung, dass 7 kein Teiler von 337 ist. Denn andernfalls wäre 7 auch ein Teiler von $2\cdot 3\cdot 5\cdot 11$, was nicht der Fall ist, denn die einzigen Primteiler dieses Produkts sind 2, 3, 5 und 11. Wären 13 oder 17 Teiler von 337, dann müsste 13 oder 17 auf Grund der Gleichung $337 = 13\cdot 17+2^2\cdot 29$ auch Teiler von $2^2\cdot 29$ sein, was ebenfalls nicht erfüllt ist, denn die einzigen Primteiler dieser Zahl sind 2 und 29. Insgesamt wird 337 also von keiner Primzahl $p \leq 17$ geteilt.

zu (b) Wegen $\bar{0}^n = \bar{0} \neq \bar{1}$ ist jede Lösung von $x^n = \bar{1}$ in $\mathbb{F}_p$ auch in $\mathbb{F}_p^\times$ enthalten. Die Ordnung jedes Elements $\alpha \in \mathbb{F}_p^\times$ ist auf jeden Fall ein Teiler von $|\mathbb{F}_p^\times| = p-1$. Darüber hinaus gilt die Äquivalenz

$$\alpha^n = \bar{1} \quad\Leftrightarrow\quad \mathrm{ord}(\alpha) \mid n \quad\Leftrightarrow\quad \mathrm{ord}(\alpha) \mid n \wedge \mathrm{ord}(\alpha) \mid (p-1) \quad\Leftrightarrow\quad \mathrm{ord}(\alpha) \mid \mathrm{ggT}(n, p-1) = 1$$
$$\Leftrightarrow\quad \alpha^{\mathrm{ggT}(n,p-1)} = \bar{1}.$$

Allgemein gilt: Ist G eine zyklische Gruppe der Ordnung m, $g \in G$ ein erzeugendes Element und d ein Teiler von m, dann ist $\langle g^d\rangle$ die eindeutig bestimmte Untergruppe von G mit Ordnung $\frac{m}{d}$, und jedes Element h mit $h^{m/d} = e_G$ ist in dieser Untergruppe enthalten. Daraus folgt, dass es in G genau $\frac{m}{d}$ Elemente h gibt, die die Gleichung $h^{m/d} = e_G$ erfüllen. Wenden wir dies auf $G = \mathbb{F}_p^\times$, $m = p-1$ und $d = \frac{p-1}{\mathrm{ggT}(n,p-1)}$ an, so kommen wir zu dem Ergebnis, dass in $\mathbb{F}_p^\times$ genau $\mathrm{ggT}(n, p-1)$ Elemente α mit $\alpha^{\mathrm{ggT}(n,p-1)} = \bar{1}$ gibt, auf Grund der Äquivalenz also ebenso viele Elemente α mit $\alpha^n = \bar{1}$.

zu (c) Die Primfaktorzerlegung von 2022 ist gegeben durch $2\cdot 3\cdot 337$. Auf Grund des Chinesischen Restsatzes existiert also ein Isomorphismus

$$\phi : \mathbb{Z}/2022\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/337\mathbb{Z}$$

von Ringen. Seien $a \in \mathbb{Z}/2022\mathbb{Z}$ und $(b, c, d) = \phi(a)$. Dann gilt für jedes $n \in \mathbb{N}$ auf Grund der Bijektivität von ϕ die Äquivalenz

$$a^n = \bar{1} \quad\Leftrightarrow\quad \phi(a^n) = \phi(\bar{1}) \quad\Leftrightarrow\quad \phi(a)^n = (\bar{1}, \bar{1}, \bar{1}) \quad\Leftrightarrow\quad (b^n, c^n, d^n) = (\bar{1}, \bar{1}, \bar{1})$$
$$\Leftrightarrow\quad b^n = \bar{1} \ \wedge\ c^n = \bar{1} \ \wedge\ d^n = \bar{1}.$$

Definieren wir für jedes $m \in \mathbb{N}$ die Menge $\mathcal{L}_m = \{a \in \mathbb{Z}/m\mathbb{Z} \mid a^n = \bar{1}\}$, dann ist durch ϕ also eine Bijektion zwischen $\mathcal{L}_{2022}$ und $\mathcal{L}_2 \times \mathcal{L}_3 \times \mathcal{L}_{337}$ gegeben. Nach Teil (b) gilt $|\mathcal{L}_p| = \mathrm{ggT}(n, p-1)$ für jede Primzahl p. Insgesamt erhalten wir also

$$\begin{aligned} |\mathcal{L}_{2022}| &= |\mathcal{L}_2 \times \mathcal{L}_3 \times \mathcal{L}_{337}| = |\mathcal{L}_2| \cdot |\mathcal{L}_3| \cdot |\mathcal{L}_{337}| = \mathrm{ggT}(n,1) \cdot \mathrm{ggT}(n,2) \cdot \mathrm{ggT}(n,336) \\ &= \mathrm{ggT}(n,2) \cdot \mathrm{ggT}(n,336). \end{aligned}$$

Gesucht werden also alle $n \in \mathbb{N}$ mit der Eigenschaft $n = \mathrm{ggT}(n,2) \cdot \mathrm{ggT}(n,336)$. Die Primfaktorzerlegung von 336 ist $2^4 \cdot 3 \cdot 7$. Weil $\mathrm{ggT}(n,2)$ ein Teiler von 2 und $\mathrm{ggT}(n,2)$ ein Teiler von 336 ist, kann $n = \mathrm{ggT}(n,2) \cdot \mathrm{ggT}(n,336)$ also nur dann erfüllt sein, wenn n ein Teiler von $2^5 \cdot 3 \cdot 7$ ist, also die Form $n = 2^a \cdot 3^b \cdot 7^c$ mit $0 \le a \le 5$ und $b, c \in \{0,1\}$ hat. Weiter gilt die Äquivalenz

$$\begin{aligned} \mathrm{ggT}(n,2) \cdot \mathrm{ggT}(n,336) = n &\quad\Leftrightarrow\quad 2^{\min\{a,1\}} \cdot 2^{\min\{a,4\}} \cdot 3^{\min\{b,1\}} \cdot 7^{\min\{c,1\}} = 2^a \cdot 3^b \cdot 7^c \\ &\Leftrightarrow\quad 2^{\min\{a,1\}+\min\{a,4\}} \cdot 3^{\min\{b,1\}} \cdot 7^{\min\{c,1\}} = 2^a \cdot 3^b \cdot 7^c \\ &\Leftrightarrow\quad \min\{a,1\} + \min\{a,4\} = a \ \wedge\ \min\{b,1\} = b \ \wedge\ c = \min\{c,1\} \\ &\overset{b,c\in\{0,1\}}{\Leftrightarrow}\quad \min\{a,1\} + \min\{a,4\} = a \quad\overset{a\in\{0,1,\ldots,5\}}{\Leftrightarrow}\quad a \in \{0,5\} \\ \Leftrightarrow\quad n \in \{2^a \cdot 3^b \cdot 7^c \mid a \in \{0,5\}, b, c \in \{0,1\}\} &\quad\Leftrightarrow\quad n \in \{1,3,7,21,32,96,224,672\}. \end{aligned}$$

Es gibt also genau acht natürliche Zahlen n mit der Eigenschaft, dass die Gleichung $x^n = \bar{1}$ genau n Lösungen in $\mathbb{Z}/2022\mathbb{Z}$ besitzt.

Aufgabe H22T2A4

Sei $f = x^6 + 3 \in \mathbb{Q}[x]$, sei $\alpha \in \mathbb{C}$ eine Nullstelle von f, und sei $K = \mathbb{Q}(\alpha) \subseteq \mathbb{C}$. Zeigen Sie:

(a) Das Polynom f ist über $\mathbb{Q}$ irreduzibel.

(b) Die Zahl $\zeta = \frac{1}{2}(1 + \alpha^3) \in K$ ist eine primitive sechste Einheitswurzel.

(c) Der Körper K ist eine Galois-Erweiterung von $\mathbb{Q}$.

(d) Die Galois-Gruppe $\mathrm{Gal}(K|\mathbb{Q})$ ist nicht abelsch.

Lösung:
zu (a) Auf Grund des Eisenstein-Kriteriums, angewendet auf die Primzahl $p = 3$, ist f irreduzibel in $\mathbb{Z}[x]$, und auf Grund des Gauß'schen Lemmas auch in $\mathbb{Q}[x]$.

zu (b) Zu zeigen ist, dass es sich bei ζ um ein Element der Ordnung 6 in der multiplikativen Gruppe $\mathbb{C}^\times$ handelt. Dafür müssen wir überprüfen, dass $\zeta^2 \neq 1$, $\zeta^3 \neq 1$ und $\zeta^6 = 1$ gilt. Zunächst bemerken wir, dass wegen $f(\alpha) = 0$ die Gleichung $\alpha^6 = -3$ gilt. Da f normiert und über $\mathbb{Q}$ irreduzibel ist und $f(\alpha) = 0$ gilt, handelt es sich bei f um das Minimalpolynom von α über $\mathbb{Q}$. Laut Vorlesung folgt daraus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \mathrm{grad}(f) = 6$, und $\{1, \alpha, ..., \alpha^5\}$ ist eine 6-elementige Basis von $\mathbb{Q}(\alpha)$ als $\mathbb{Q}$-Vektorraum. Dies bedeutet, dass zwei Elemente $\sum_{j=0}^5 b_j\alpha^j$ und $\sum_{j=0}^5 c_j\alpha^j$ mit $b_j, c_j \in \mathbb{Q}$ für $0 \leq j \leq 5$ genau dann übereinstimmen, wenn $b_j = c_j$ für $0 \leq j \leq 5$ gilt.

Die Rechnungen $\zeta^2 = \frac{1}{4}(1 + \alpha^3)^2 = \frac{1}{4}(1 + 2\alpha^3 + \alpha^6) = \frac{1}{4}(1 + 2\alpha^3 + (-3)) = -\frac{1}{2} + \frac{1}{2}\alpha^3$ und $\zeta^3 = \zeta \cdot \zeta^2 = \frac{1}{2}(1 + \alpha^3) \cdot \frac{1}{2}(-1 + \alpha^3) = \frac{1}{4}(-1 - \alpha^3 + \alpha^3 + \alpha^6) = \frac{1}{4}(-1 - 3) = -1$ zeigen also, dass ζ^2 und ζ^3 ungleich 1 sind. Andererseits gilt $\zeta^6 = (\zeta^3)^2 = (-1)^2 = 1$.

zu (c) Die Erweiterung $K|\mathbb{Q}$ ist algebraisch, weil das Element α als Nullstelle des Polynoms $0 \neq f \in \mathbb{Q}[x]$ algebraisch über $\mathbb{Q}$ ist und weil K der vom algebraischen Element α erzeugte Zwischenkörper der Erweiterung $\mathbb{C}|\mathbb{Q}$ ist. Wegen $\mathrm{char}(K|\mathbb{Q}) = 0$ ist diese algebraische Erweiterung auch separabel. Nun zeigen wir noch, dass $K|\mathbb{Q}$ normal ist, indem wir nachweisen, dass K in $\mathbb{C}$ mit dem Zerfällungskörper von f über $\mathbb{Q}$ übereinstimmt. Wegen $f(0) \neq 0$ ist $\alpha \neq 0$. Weil ζ nach Teil (b) eine primitive sechste Einheitswurzel ist, sind die Elemente ζ^j für $0 \leq j \leq 5$ paarweise verschieden, und wegen $\alpha \neq 0$ gilt dasselbe für die Elemente $\zeta^j\alpha$ mit $0 \leq j \leq 5$. Für diese j gilt jeweils $f(\zeta^j\alpha) = (\zeta^j\alpha)^6 + 3 = (\zeta^6)^j\alpha^6 + 3 = \alpha^6 + 3 = f(\alpha) = 0$, die Elemente sind also Nullstellen von f. Wegen $\mathrm{grad}(f) = 6$ kann es keine weiteren Nullstellen geben.

Dies zeigt, dass durch $N = \{\zeta^j\alpha \mid 0 \leq j \leq 5\}$ die Menge aller komplexen Nullstellen von f gegeben und $\mathbb{Q}(N)$ somit der Zerfällungskörper von f über $\mathbb{Q}$ ist. Wegen $\alpha \in N$ gilt $K = \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(N)$. Andererseits liegen die Elemente $\zeta^j\alpha$ für $0 \leq j \leq 5$ wegen $\zeta = \frac{1}{2}(1 + \alpha^3)$ alle in $K = \mathbb{Q}(\alpha)$. Aus $N \subseteq K$ folgt $\mathbb{Q}(N) \subseteq K$, insgesamt also $\mathbb{Q}(N) = K$.

zu (d) *1. Möglichkeit: Angabe einer nicht-normalen Teilerweiterung*
Wäre die Gruppe $\mathrm{Gal}(K|\mathbb{Q})$ abelsch, dann wäre jede Untergruppe von $\mathrm{Gal}(K|\mathbb{Q})$ ein Normalteiler. Nach den Sätzen der Galoistheorie würde daraus folgen, dass jeder Zwischenkörper M von $K|\mathbb{Q}$ normal über $\mathbb{Q}$ ist.

Wir führen die Annahme zu einem Widerspruch, indem wir zeigen, dass es sich bei $M = \mathbb{Q}(\sqrt[3]{3})$ um einen Zwischenkörper von $K|\mathbb{Q}$ handelt, der nicht normal über $\mathbb{Q}$ ist. Wegen $\alpha^6 = -3$ gilt $(\alpha^2)^3 = -3$, das Element α^2 ist also eine Nullstelle des Polynoms $g = x^3 + 3 \in \mathbb{Q}[x]$. Weil ζ eine primitive sechste Einheitswurzel ist, ist ζ^2 eine primitive dritte Einheitswurzel. Die Elemente 1, ζ^2, ζ^4 sind somit paarweise

verschieden, und wegen $\alpha^2 \neq 0$ gilt dasselbe für die Elemente α^2, $\zeta^2\alpha^2$ und $\zeta^4\alpha^2$. Diese drei Elemente sind die komplexen Nullstellen des Polynoms g, denn es gilt $g(\zeta^{2j}\alpha^2) = (\zeta^{2j})^3(\alpha^2)^3 + 3 = (\zeta^6)^j\alpha^6 + 3 = 1^j \cdot (-3) + 3 = 0$ für $j = 0, 1, 2$. Da offenbar $-\sqrt[3]{3} \in \mathbb{R}$ eine Nullstelle von g ist, stimmt diese mit einem der drei Elemente α^2, $\zeta^2\alpha^2$ und $\zeta^4\alpha^2$ überein.

Es gilt also $\sqrt[3]{3} \in K$, und somit ist $M = \mathbb{Q}(\sqrt[3]{3})$ tatsächlich ein Zwischenkörper von $K|\mathbb{Q}$. Auf Grund des Eisenstein-Kriteriums (angwendet auf die Primzahl 3) und des Gauß'schen Lemmas ist das Polynom g irreduzibel über g, und es besitzt in M die Nullstelle $\sqrt[3]{3}$. Wäre $M|\mathbb{Q}$ eine normale Erweiterung, dann müsste g über M in Linearfaktoren zerfallen und somit auch die beiden anderen komplexen Nullstellen in M liegen. Aber dies ist nicht der Fall. Denn wegen $\sqrt[3]{3} \in \mathbb{R}$ ist M ein Teilkörper von $\mathbb{R}$. Die beiden von $\sqrt[3]{3}$ verschiedenen Nullstellen des Polynoms g sind aber $\zeta^2\sqrt[3]{3}$ und $\zeta^4\sqrt[3]{3}$, und diese sind nicht reell, weil die beiden primitiven dritten Einheitswurzeln, also die Elemente der Menge $\{\zeta^2, \zeta^4\} = \{-\frac{1}{2} \pm \sqrt{1}2\sqrt{-3}\}$, nicht in $\mathbb{R}$ liegen. Also ist $M|\mathbb{Q}$ keine normale Erweiterung.

2. Möglichkeit: direkter Nachweis der Nicht-Kommutativität
Nach Teil (a) ist f irreduzibel über $\mathbb{Q}$, und wie in Teil (c) festgestellt wurde, sind unter anderen $\pm\alpha$ und $\zeta^2\alpha$ Nullstellen von f in K. Auf Grund des Fortsetzungssatzes gibt es somit Elemente $\sigma, \tau \in \mathrm{Gal}(K|\mathbb{Q})$ mit $\sigma(\alpha) = -\alpha$ und $\tau(\alpha) = \zeta\alpha$. In Teil (b) hatten wir nachgerechnet, dass $\zeta^2 = -\frac{1}{2} + \frac{1}{2}\alpha^3$ und $\zeta^3 = -1$ gilt. Wegen $\zeta = \frac{1}{2}(1 + \alpha^3)$ erhalten wir damit

$$\sigma(\zeta) \quad = \quad \sigma(\tfrac{1}{2}(1+\alpha^3)) \quad = \quad \tfrac{1}{2}(1+\sigma(\alpha)^3) \quad = \quad \tfrac{1}{2}(1+(-\alpha)^3) \quad = \quad \tfrac{1}{2}(1-\alpha^3) \quad = \quad -\zeta^2$$

und ebenso

$$\tau(\zeta) \quad = \quad \tau(\tfrac{1}{2}(1+\alpha^3)) \quad = \quad \tfrac{1}{2}(1+\tau(\alpha)^3) \quad = \quad \tfrac{1}{2}(1+(\zeta\alpha)^3) \quad = \quad \tfrac{1}{2}(1-\alpha^3) \quad = \quad -\zeta^2.$$

Damit erhalten wir einerseits

$$(\sigma \circ \tau)(\alpha) \quad = \quad \sigma(\tau(\alpha)) \quad = \quad \sigma(\zeta\alpha) \quad = \quad \sigma(\zeta)\sigma(\alpha) \quad = \quad (-\zeta^2)(-\alpha) \quad = \quad \zeta^2\alpha$$

andererseits aber

$$(\tau \circ \sigma)(\alpha) \quad = \quad \tau(\sigma(\alpha)) \quad = \quad \tau(-\alpha) \quad = \quad -\tau(\alpha) \quad = \quad -\zeta\alpha \quad = \quad \zeta^4\alpha.$$

Weil ζ nach Teil (b) eine primitive sechste Einheitswurzel ist, gilt $\zeta^2 \neq \zeta^4$ und somit auch $(\sigma \circ \tau)(\alpha) \neq (\tau \circ \sigma)(\alpha)$ und $\sigma \circ \tau \neq \tau \circ \sigma$. Dies zeigt, dass die Gruppe $\mathrm{Gal}(K|\mathbb{Q})$ tatsächlich nicht kommutativ ist.

Aufgabe H22T2A5

Sei G eine Gruppe der Ordnung 2022.

(a) Nennen Sie vier paarweise nicht isomorphe Beispiele von Gruppen der Ordnung 2022 und begründen Sie, dass die Gruppen paarweise nicht isomorph sind.

(b) Zeigen Sie, dass G auflösbar ist.

(c) Beweisen Sie, dass G einen Normalteiler vom Index 2 besitzt.

Lösung:
zu (a) Sei $G_1 = \mathbb{Z}/2022\mathbb{Z}$, $G_2 = D_{1011}$ (die Diedergruppe mit $2 \cdot 1011 = 2022$ Elementen), $G_3 = S_3 \times \mathbb{Z}/337\mathbb{Z}$ und $G_4 = \mathbb{Z}/3\mathbb{Z} \times D_{337}$. Weil S_3, D_{337} und D_{1011} nicht-abelsche Gruppen sind, gilt dasselbe für G_2, G_3 und G_4. Weil die Gruppe G_1 abelsch ist, ist sie zu keiner der drei anderen Gruppen isomorph. Die Gruppe D_{1011} besitzt genau 1011 Elemente der Ordnung 2. (Dies sind die Spiegelungen in der Symmetriegruppe des regelmäßigen 1011-Ecks. Es gibt keine Drehung von Ordnung 2, weil 1011 ungerade ist.)

Wir zeigen nun, dass G_3 genau drei und G_4 genau 337 Elemente der Ordnung 2 besitzt. Weil die Anzahlen der Elemente der Ordnung 2 in den drei Gruppen G_2, G_3, G_4 nicht übereinstimmen, sind auch diese paarweise nicht-isomorph. Für jedes Element $(\sigma, a) \in G_3$ (mit $\sigma \in S_3$ und $a \in \mathbb{Z}/337\mathbb{Z}$) gilt die Äquivalenz

$$\begin{aligned}\operatorname{ord}(\sigma,a) = 2 \quad &\Leftrightarrow \quad (\sigma,a)^2 = e_{G_3} \ \wedge \ (\sigma,a) \neq e_{G_3} \quad \Leftrightarrow \quad (\sigma^2, \bar{2}a) = (\mathrm{id}, \bar{0}) \ \wedge \ (\sigma,a) \neq (\mathrm{id},\bar{0}) \\ &\Leftrightarrow \quad (\sigma^2, a) = (\mathrm{id},\bar{0}) \ \wedge \ (\sigma,a) \neq (\mathrm{id},\bar{0}) \quad \Leftrightarrow \quad a = \bar{0} \ \wedge \ \sigma \in \{(1\ 2), (2\ 3), (1\ 3)\} \\ &\Leftrightarrow \quad (\sigma,a) \in \{((1\ 2),\bar{0}), ((2\ 3),\bar{0}), ((1\ 3),\bar{0})\}.\end{aligned}$$

Dabei wurde im dritten Schritt verwendet, dass $\bar{2}$ wegen $\mathrm{ggT}(2, 337) = 1$ in $\mathbb{Z}/337\mathbb{Z}$ invertierbar ist und somit $\bar{2}a = \bar{0}$ äquivalent zu $a = \bar{0}$ ist. Im vierten Schritt haben wir verwendet, dass die Elemente $\sigma \in S_3$ mit $\sigma^2 = \mathrm{id}$ und $\sigma \neq \mathrm{id}$ durch $(1\ 2), (2\ 3), (1\ 3)$ gegeben sind. Insgesamt zeigt die Rechnung, dass es in G_3 tatsächlich genau drei Elemente der Ordnung 2 gibt.

Für alle $(a, \sigma) \in G_4$ mit $a \in \mathbb{Z}/3\mathbb{Z}$ und $\sigma \in D_{337}$ gilt die Äquivalenz

$$\begin{aligned}&\operatorname{ord}(a,\sigma) = 2 \quad \Leftrightarrow \quad (a,\sigma)^2 = (\bar{0},\mathrm{id}) \ \wedge \ (a,\sigma) = (\bar{0},\mathrm{id}) \quad \Leftrightarrow \quad (\bar{2}a, \sigma^2) = (\bar{0},\mathrm{id}) \ \wedge \ (a,\sigma) = (\bar{0},\mathrm{id}) \\ &\Leftrightarrow \quad (a,\sigma^2) = (\bar{0},\mathrm{id}) \ \wedge \ (a,\sigma) = (\bar{0},\mathrm{id}) \quad \Leftrightarrow \quad a = \bar{0} \ \wedge \ \sigma^2 = \mathrm{id} \ \wedge \ \sigma \neq \mathrm{id} \quad \Leftrightarrow \quad a = \bar{0} \ \wedge \ \operatorname{ord}(\sigma) = 2.\end{aligned}$$

In D_{337} gibt es genau 337 Elemente der Ordnung 2. Also zeigt die Rechnung, dass es ebenso viele Elemente der Ordnung 2 in G_4 gibt.

zu (b) Sei G eine Gruppe der Ordnung $2022 = 2 \cdot 3 \cdot 337$. (Die Zahl 337 ist eine Primzahl.) Für jede Primzahl p sei ν_p die Anzahl der p-Sylowgruppen von G. Auf Grund des Dritten Sylowsatzes gilt $\nu_{337} \mid 2 \cdot 3$, also $\nu_{337} \in \{1, 2, 3, 6\}$. Außerdem gilt $\nu_{337} \equiv 1 \bmod 337$. Wegen $2, 3, 6 \not\equiv 1 \bmod 337$ folgt $\nu_{337} = 1$. Sei N die einzige 337-Sylowgruppe von G. Wegen $\nu_{337} = 1$ gilt $N \trianglelefteq G$. Laut Vorlesung ist G auflösbar, wenn N und G/N beide auflösbar sind. Die Gruppe N ist auf Grund der Primzahlordnung $|N| = 337$ zyklisch, damit auch abelsch und auflösbar. Es bleibt zu zeigen, dass G/N eine auflösbare Gruppe ist.

Auf Grund des Satzes von Lagrange gilt $|G/N| = (G : N) = \frac{|G|}{|N|} = \frac{2022}{337} = 6$. Sei $\bar{P}$ ein beliebige 3-Sylowgruppe von $\bar{G} = G/N$. Dann gilt $|\bar{P}| = 3$ und $(\bar{G} : \bar{P}) = \frac{6}{3} = 2$. Als Untergruppe vom Index 2 ist $\bar{P}$ ein Normalteiler von $\bar{G}$. Als Gruppen der Primzahlordnungen $|\bar{P}| = 3$ und $|\bar{G}/\bar{P}| = (\bar{G} : \bar{P}) = 2$ sind $\bar{P}$ und $\bar{G}/\bar{P}$ beide zyklisch und damit auch auflösbar. Dies zeigt, dass auch $\bar{G}$ eine auflösbare Gruppe ist.

zu (c) In Teil (b) wurde gezeigt, dass G einen Normalteiler N von Ordnung 337 besitzt. Sei $\pi_N : G \to G/N$ der kanonische Epimorphismus. Aus der Korrespondenzsatz für Gruppen folgt: Ist $\bar{U}$ eine Untergruppe von G/N vom Index $d \in \mathbb{N}$, dann ist $U = \pi_N^{-1}(\bar{U})$ eine Untergruppe vom Index d von G mit $U \supseteq N$. In Teil (b) haben wir auch gezeigt, dass in G/N eine Untergruppe $\bar{P}$ vom Index 2 existiert. Also ist $P = \pi_N^{-1}(\bar{P})$ eine Untergruppe vom Index 2 von G. Wegen $(G : P) = 2$ handelt es sich darüber hinaus um einen Normalteiler.

Aufgabe H22T3A1

Gegeben sei eine endliche Körpererweiterung $L|K$. Weiterhin sei $\mathrm{Tr}_{L|K} : L \to K$ die Abbildung, die jeden Element $a \in L$ die Spur der Multiplikation $m_a : L \to L$, $b \mapsto ab$ zuordnet. Dabei ist die *Spur* einer K-linearen Abbildung $\varphi : L \to L$ definiert als die Summe der Hauptdiagonalelemente einer Darstellungsmatrix.

(a) Zeigen Sie, dass $\mathrm{Tr}_{L|K}$ eine K-lineare Abbildung ist.

(b) Nun sei $\{a_1, ..., a_n\}$ eine K-Basis von L. Beweisen Sie, dass sich die *Diskriminante* $\Delta_{L|K}(a_1, ..., a_n) = \det(\mathrm{Tr}(\alpha_i\alpha_j)_{ij})$ um einen Faktor aus $(K^\times)^2$ ändert, wenn man die Basis wechselt.

(c) Seien $p, q \in \mathbb{Q}$ so gewählt, dass $f = x^2 + px + q$ ein irreduzibles Polynom ist. Finden Sie $\Delta_{L|K}(1, \alpha)$ für $K = \mathbb{Q}$ und $L = K[x]/(f)$, wobei α die Restklasse von x in L bezeichne.

Lösung:
zu (a) Sei $n = [L : K] = \dim_K L$ und $\mathcal{B} = (\alpha_1, ..., \alpha_n)$ eine geordnete Basis von L als K-Vektorraum. Für jedes $\phi \in \mathrm{End}_K(L)$ sei $\mathcal{M}_\mathcal{B}(\phi)$ die Darstellungsmatrix von ϕ bezüglich $\mathcal{B}$. Für jede Matrix $A = (a_{ij}) \in \mathcal{M}_{n,K}$ sei $\mathrm{Tr}(A) = \sum_{i=1}^n a_{ii}$ die Spur. Nach Definition gilt $\mathrm{Tr}_{L|K}(a) = \mathrm{Tr}(\mathcal{M}_\mathcal{M}(m_a))$ für alle $a \in L$. Für den Nachweis, dass $\mathrm{Tr}_{L|K} : L \to K$ eine lineare Abbildung ist, genügt es zu überprüfen

(1) Die Abbildung $L \to \mathrm{End}_K(L)$, $a \mapsto m_a$ ist linear.

(2) Die Abbildung $\mathrm{End}_K(L) \to \mathcal{M}_{n,K}$, $\phi \mapsto \mathcal{M}_\mathcal{B}(\phi)$ ist linear.

(3) Die Abbildung $\mathrm{Tr} : \mathcal{M}_{n,K} \to K$, $A \mapsto \mathrm{Tr}(A)$ ist linear.

zu (1) Seien $a, a' \in L$ und $\lambda \in K$ vorgegeben. Zu überprüfen sind die beiden Gleichungen $m_{a+a'} = m_a + m_{a'}$ und $m_{\lambda a} = \lambda m_a$ in $\mathrm{End}_K(L)$. Sei dazu b ein beliebiges Element aus L. Es gilt

$$m_{a+a'}(b) \quad = \quad (a + a')b \quad = \quad ab + a'b \quad = \quad m_a(b) + m_{a'}(b) \quad = \quad (m_a + m_{a'})(b)$$

und ebenso $m_{\lambda a}(b) = (\lambda a)b = \lambda(ab) = \lambda m_a(b) = (\lambda m_a)(b)$. Damit sind die beiden Gleichungen in $\mathrm{End}_K(L)$ verifziert.

zu (2) Laut Vorlesung gilt: Sind V, W zwei K-Vektorräume der endlichen Dimensionen $n = \dim V$ und $m = \dim W$, ist $\mathcal{A}$ eine geordnete Basis von V und $\mathcal{B}$ eine geordnete Basis von W, dann ist durch $\mathrm{Hom}_K(V, W) \to \mathcal{M}_{m\times n,K}$, $\phi \mapsto \mathcal{M}_\mathcal{B}^\mathcal{A}(\phi)$ ein Isomorphismus von K-Vektorräumen definiert, insbesondere eine linearen Abbildung. Anwendung dieser Aussage auf $V = W = L$ und die Basis $\mathcal{B}$ liefert die angegebene Behauptung.

zu (3) Seien $A = (a_{ij})$ und $B = (b_{ij})$ Elemente des K-Vektorraums $\mathcal{M}_{n,K}$, und sei $\lambda \in K$. Dann gilt

$$\mathrm{Tr}(A + B) \quad = \quad \sum_{i=1}^n (a_{ii} + b_{ii}) \quad = \quad \sum_{i=1}^n a_{ii} + \sum_{i=1}^n b_{ii} \quad = \quad \mathrm{Tr}(A) + \mathrm{Tr}(B)$$

und ebenso $\mathrm{Tr}(\lambda A) = \sum_{i=1}^n (\lambda a_{ii}) = \lambda \sum_{i=1}^n a_{ii} = \lambda \mathrm{Tr}(A)$.

zu (b) Diese Aussage beweisen wir durch Anwendung des Satzes vom Basiswechsel für Bilinearformen. Zunächst überprüfen wir, dass durch $b : L \times L \to K$, $(\alpha, \beta) \mapsto \mathrm{Tr}_{L|K}(\alpha\beta)$ eine Bilinearform auf L definiert ist. Seien $\alpha, \alpha', \beta, \beta' \in L$ und $\lambda \in K$ vorgegeben. Dann gilt

$$\begin{aligned}
b(\alpha+\alpha',\beta) &= \mathrm{Tr}_{L|K}((\alpha+\alpha')\beta) = \mathrm{Tr}_{L|K}(\alpha\beta+\alpha'\beta) = \mathrm{Tr}_{L|K}(\alpha\beta)+\mathrm{Tr}_{L|K}(\alpha'\beta) = b(\alpha,\beta)+b(\alpha',\beta)\\
b(\alpha,\beta+\beta') &= \mathrm{Tr}_{L|K}(\alpha(\beta+\beta')) = \mathrm{Tr}_{L|K}(\alpha\beta+\alpha\beta') = \mathrm{Tr}_{L|K}(\alpha\beta')+\mathrm{Tr}_{L|K}(\alpha\beta') = b(\alpha,\beta)+b(\alpha,\beta')\\
b(\lambda\alpha,\beta) &= \mathrm{Tr}_{L|K}(\lambda\alpha\beta) = \lambda\mathrm{Tr}_{L|K}(\alpha\beta) = \lambda b(\alpha,\beta)\\
b(\alpha,\lambda\beta) &= \mathrm{Tr}_{L|K}(\lambda\alpha\beta) = \lambda\mathrm{Tr}_{L|K}(\alpha\beta) = \lambda b(\alpha,\beta).
\end{aligned}$$

Also ist durch b tatsächlich eine Bilinearform auf dem K-Vektorraum L definiert. Seien $\mathcal{A} = (\alpha_1, ..., \alpha_n)$ und $\mathcal{A}' = (\alpha'_1, ..., \alpha'_n)$ zwei geordnete Basen von L. Dann sind die Darstellungsmatrizen von b bezüglich $\mathcal{A}$ und $\mathcal{A}'$ gegeben durch

$$\mathcal{M}_{\mathcal{A}}(b) = (\mathrm{Tr}_{L|K}(\alpha_i\alpha_j))_{ij} \qquad \text{und} \qquad \mathcal{M}_{\mathcal{A}'}(b) = (\mathrm{Tr}_{L|K}(\alpha'_i\alpha'_j))_{ij}.$$

Nach dem Satz vom Basiswechsel für Bilinearformen gilt

$$\mathcal{M}_{\mathcal{A}'}(b) = {}^{\mathrm{t}}\mathcal{T}_{\mathcal{A}}^{\mathcal{A}'} \cdot \mathcal{M}_{\mathcal{A}}(b) \cdot \mathcal{T}_{\mathcal{A}}^{\mathcal{A}'}$$

wobei $\mathcal{T}_{\mathcal{A}}^{\mathcal{A}'}$ die Matrix des Basiswechsels von $\mathcal{A}'$ nach $\mathcal{A}$ bezeichnet. Sei $c = \det \mathcal{T}_{\mathcal{A}}^{\mathcal{A}'} \in K$. Weil die Matrix $\mathcal{T}_{\mathcal{A}}^{\mathcal{A}'}$ invertierbar ist, liegt $c \in K^\times$. Die zu beweisende Aussage aus der Aufgabenstellung ergibt sich nun durch die Rechnung

$$\begin{aligned}
\Delta_{L|K}(\mathcal{A}') &= \det\left(\mathrm{Tr}_{L|K}(\alpha'_i\alpha'_j)\right) = \det \mathcal{M}_{\mathcal{A}'}(b) = \det\left({}^{\mathrm{t}}\mathcal{T}_{\mathcal{A}}^{\mathcal{A}'}\mathcal{M}_{\mathcal{A}'}(b)\mathcal{T}_{\mathcal{A}}^{\mathcal{A}'}\right)\\
&= (\det \mathcal{T}_{\mathcal{A}}^{\mathcal{A}'})^2 \cdot \det \mathcal{M}_{\mathcal{A}}(b) = c^2 \det\left(\mathrm{Tr}_{L|K}(\alpha_i\alpha_j)\right) = c^2\Delta_{L|K}(\mathcal{A}).
\end{aligned}$$

zu (c) Wir berechnen die Darstellungsmatrizen A_β von m_β bezüglich der Basis $\mathcal{B} = (1, \alpha)$ des K-Vektorraums L, für $\beta \in \{1, \alpha, \alpha^2\}$. Zur Vorbereitung berechnen wir

$$\begin{aligned}
\alpha^2 &= (x+(f))^2 = x^2+(f) = x^2 - f + (f) = x^2 - (x^2+px+q) + (f)\\
&= -px - q + (f) = (-p+(f))(x+(f)) - (q+(f)) = -p\alpha - q\\
\alpha^3 &= \alpha\cdot\alpha^2 = \alpha(-p\alpha - q) = -p\alpha^2 - q\alpha = -p(-p\alpha-q) - q\alpha = (p^2-q)\alpha + pq
\end{aligned}$$

Nun gilt $m_1(1) = 1 \cdot 1 = 1 \cdot 1 + 0 \cdot \alpha$, $m_1(\alpha) = \alpha = 0 \cdot 1 + 1 \cdot \alpha$. Dies liefert die Darstellungsmatrix

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

und $\mathrm{Tr}_{L|\mathbb{Q}}(1) = \mathrm{Tr}(A_1) = 1 + 1 = 2$. Die Gleichungen $m_\alpha(1) = \alpha = 0 \cdot 1 + 1 \cdot \alpha$ und $m_\alpha(\alpha) = \alpha^2 = (-q) \cdot 1 + (-p) \cdot \alpha$ liefern die Darstellungsmatrix

$$A_\alpha = \begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix}$$

und $\mathrm{Tr}_{L|\mathbb{Q}}(\alpha) = \mathrm{Tr}(A_\alpha) = 0 + (-p) = -p$. Die Gleichungen $m_{\alpha^2}(1) = \alpha^2 = (-q) \cdot 1 + (-p) \cdot \alpha$ und $m_{\alpha^2}(\alpha) = \alpha^3 = (pq) \cdot 1 + (p^2 - q) \cdot \alpha$ liefern schließlich die Darstellungsmatrix

$$A_{\alpha^2} = \begin{pmatrix} -q & pq \\ -p & p^2-q \end{pmatrix}$$

und $\mathrm{Tr}_{L|\mathbb{Q}}(\alpha^2) = \mathrm{Tr}(A_{\alpha^2}) = (-q) + (p^2 - q) = p^2 - 2q$.

Für die Diskriminante erhalten wir nun

$$\begin{aligned}\Delta_{L|\mathbb{Q}}(1,\alpha) &= \det\begin{pmatrix}\mathrm{Tr}_{L|\mathbb{Q}}(1) & \mathrm{Tr}_{L|\mathbb{Q}}(\alpha)\\ \mathrm{Tr}_{L|\mathbb{Q}}(\alpha) & \mathrm{Tr}_{L|\mathbb{Q}}(\alpha^2)\end{pmatrix} = \det\begin{pmatrix}2 & -p\\ -p & p^2-2q\end{pmatrix}\\ &= 2(p^2-2q)-(-p)^2 = p^2-4q.\end{aligned}$$

Aufgabe H22T3A2

(a) Geben Sie eine vollständige Definition des kleinsten gemeinsamen Vielfachen zweier ganzer Zahlen an.

(b) Beweisen Sie mit Hilfe Ihrer Definition aus (a), dass für $a, b, c, d \in \mathbb{Z}$ die folgende Formel gilt:

$$\mathrm{kgV}(\mathrm{kgV}(a,b), \mathrm{kgV}(c,d)) \ , \ \mathrm{kgV}(\mathrm{kgV}(a,c), \mathrm{kgV}(b,d)).$$

Lösung:
zu (a) Seien $a, b \in \mathbb{Z}$. Dann ist $\mathrm{kgV}(a,b)$ die eindeutig bestimmte Zahl $d \in \mathbb{N}_0$ mit den folgenden beiden Eigenschaften.

(i) $a \mid d$ und $b \mid d$

(ii) Für alle $d' \in \mathbb{N}_0$ folgt aus $a \mid d'$ und $b \mid d'$ jeweils $d \mid d'$.

Damit ist die Zahl eindeutig bestimmt. Erfüllen nämlich d und d' aus $\mathbb{N}_0$ beide die Bedingungen (i) und (ii), dann gilt $d \mid d'$ und $d' \mid d$, und wegen $d, d' \in \mathbb{N}_0$ folgt daraus $d = d'$.

zu (b) Seien $a, b, c, d \in \mathbb{Z}$ vorgegeben, und sei $r = \mathrm{kgV}(\mathrm{kgV}(a,b), \mathrm{kgV}(c,d))$. Wir zeigen, dass r die definierenden Bedingungen (i) und (ii) des kgV von $\mathrm{kgV}(a,c)$ und $\mathrm{kgV}(b,d)$ erfüllt. Es gilt $\mathrm{kgV}(a,b) \mid r$ und $\mathrm{kgV}(c,d) \mid r$. Daraus wiederum folgt $a \mid r$, $b \mid r$, $c \mid r$ und $d \mid r$. Aus $a \mid r$ und $c \mid r$ folgt $\mathrm{kgV}(a,c) \mid r$, und aus $b \mid r$ und $d \mid r$ folgt ebenso $\mathrm{kgV}(b,d) \mid r$. Damit ist Bedingung (i) verifiziert.

Sei nun $s \in \mathbb{N}_0$ mit $\mathrm{kgV}(a,c) \mid s$ und $\mathrm{kgV}(b,d) \mid s$. Dann folgt $a \mid s$, $c \mid s$, $b \mid s$ und $d \mid s$. Aus $a \mid s$ und $b \mid s$ folgt $\mathrm{kgV}(a,b) \mid s$. Aus $c \mid s$ und $d \mid s$ folgt $\mathrm{kgV}(c,d) \mid s$. Aus $\mathrm{kgV}(a,b) \mid s$ und $\mathrm{kgV}(c,d) \mid s$ wiederum folgt $r \mid s$, auf Grund von Bedingung (ii) für das kleinste gemeinsame Vielfache von $\mathrm{kgV}(a,b)$ und $\mathrm{kgV}(c,d)$. Damit ist Bedingung (ii) für das kleinste gemeinsame Vielfache von $\mathrm{kgV}(a,c)$ und $\mathrm{kgV}(b,d)$ nachgewiesen.

Anmerkung:

Für $a, b \in \mathbb{Z}$ gilt $\mathrm{kgV}(a,b) = 0$ genau dann, wenn $a = 0$ oder $b = 0$ ist. Ist nämlich $a = 0$ und setzen wir und setzen wir $d = \mathrm{kgV}(a,b)$, so gilt $a \mid d$, also $d = ka$ für ein $k \in \mathbb{Z}$. Es folgt $d = k \cdot 0 = 0$. Ebenso folgt aus $b = 0$, dass $\mathrm{kgV}(a,b) = 0$ ist. Sind andererseits a und b beide ungleich null, dann ist $|ab| \in \mathbb{N}$ ein gemeinsames Vielfaches von a und b. Also muss $d = \mathrm{kgV}(a,b)$ ein Teiler von $|ab|$ sein. Dies ist nur möglich, wenn d ungleich null ist, denn 0 ist kein Teiler einer ganzen Zahl ungleich 0.

Weder in Teil (a) noch in Teil (b) ist es notwendig, die Situation, dass eine der Zahlen a, b, c, d gleich 0 ist, als Sonderfall zu betrachten.

Aufgabe H22T3A3

Seien p, q, r Primzahlen mit $p < q < r$, und sei G eine Gruppe der Ordnung pqr. Für $i \in \{p, q, r\}$ bezeichne ν_i die Anzahl der verschiedenen i-Sylowgruppen von G. Beweisen Sie:

(a) Besitzt G keine normale Sylowgruppe, so gilt $\nu_p \geq q$ und $\nu_q \geq r$ und $\nu_r = pq$.

(b) Die Gruppe G besitzt eine normale Sylowgruppe.

(c) Eine Gruppe der Ordnung 2022 ist nicht einfach.

Lösung:
zu (a) Nach dem Dritte Sylowsatz gilt $\nu_p \mid (qr)$, also $\nu_p \in \{1, q, r, qr\}$. Da G keine normale p-Sylowgruppe besitzt, ist $\nu_p = 1$ ausgeschlossen. Wegen $r > q$ und $qr > q$ folgt aus $\nu_p \in \{q, r, qr\}$ direkt $\nu_p \geq q$.

Ebenso gilt $\nu_q \mid (pr)$ auf Grund des Dritten Sylowsatzes, also $\nu_q \in \{1, p, r, pr\}$. Da es keine normale q-Sylowgruppe in G gibt, gilt $\nu_q \neq 1$. Nehmen wir an, es ist $\nu_q = p$. Wegen $\nu_q \equiv 1 \bmod q$ folgt dann $p \equiv 1 \bmod q$, also $q \mid (p-1)$ und insbesondere $q < p$. Aber dies steht zur Voraussetzung $q > p$ im Widerspruch. Also gilt $\nu_q \in \{r, pr\}$, und wegen $pr > r$ folgt $\nu_q \geq r$.

Eine erneute Anwendung des Dritten Sylowsatzes liefert $\nu_r \mid (pq)$, also $\nu_r \in \{1, p, q, pq\}$. Da G keine normale r-Sylowgruppe besitzt, gilt $\nu_r \neq 1$. Aus $\nu_r = p$ oder $\nu_r = q$ würde $p \equiv 1 \bmod r$ oder $q \equiv 1 \bmod r$ folgen, also auch $r|(p-1)$ oder $r|(q-1)$ bzw. $r < p$ oder $r < q$, im Widerspruch zu den Voraussetzungen $r > q > p$. Also ist $\nu_r = pq$ die einzige verbleibende Möglichkeit.

zu (b) Nehmen wir an, G besitzt keine normale Sylowgruppe. Nach Teil (a) gilt dann $\nu_p \geq q$, $\nu_q \geq r$ und $\nu_r = pq$. Wegen $|G| = p^1 \cdot q^1 \cdot r^1$ sind die p- bzw. q- bzw. r-Sylowgruppen genau die Untergruppen der Ordnung p bzw. q bzw. r von G. Jedes Element $g \in G$ der Ordnung r liegt genau in einer r-Sylowgruppe von G, nämlich $\langle g \rangle$. Umgekehrt ist jede r-Sylowgruppe als Untergruppe der Primzahlordnung r zyklisch und enthält somit genau $\varphi(r) = r - 1$ Elemente der Ordnung $r - 1$. Insgesamt zeigt dies, dass die Anzahl der Elemente der Ordnung r in G genau $(r-1)$-mal so groß ist wie die Anzahl ν_r der r-Sylowgruppen. Es gibt also genau $pq(r-1)$ Elemente der Ordnung r in G.

Genauso folgt aus $\nu_p \geq q$, dass es in G mindestens $(p-1)q$ Elemente der Ordnung p, und aus $\nu_q \geq r$, dass es in G mindestens $(q-1)r$ Elemente der Ordnung q gibt. Insgesamt enthält G also mindestens $pq(r-1) + (p-1)q + (q-1)r$ Elemente ungleich dem Neutralelement. Wegen $|G| = pqr$ folgt

$$pq(r-1) + (p-1)q + (q-1)r + 1 \leq pqr \quad \Leftrightarrow \quad -pq + (p-1)q + (q-1)r + 1 \leq 0 \quad \Leftrightarrow$$
$$-q + (q-1)r + 1 \leq 0 \quad \Leftrightarrow \quad qr + 1 \leq q + r \quad \Leftrightarrow \quad q(r-1) + 1 \leq r.$$

Wegen $q \geq 3$ folgt daraus $3(r-1) + 1 \leq r$, was zu $3r + 1 \leq r + 3$ und $r \leq 1$ umgeformt werden kann. Aber dies steht im Widerspruch dazu, dass r eine Primzahl ist. Dies zeigt, dass es in G eine normale Sylowgruppe geben muss.

zu (c) Sei G eine Gruppe der Ordnung $2022 = 2 \cdot 3 \cdot 337$. Die Zahl 337 ist eine Primzahl, also ist $|G| = pqr$ mit den Primzahlen $p = 2 < q = 3 < r = 337$ erfüllt. Nach Teil (b) besitzt G also eine normale p-, q- oder r-Sylowgruppe. Wegen $1 < p, q, r < |G|$ handelt es sich dabei um einen nichttrivialen Normalteiler von G. Dies zeigt, dass G keine einfache Gruppe ist.

Aufgabe H22T3A4

Sei $K = \mathbb{Z}[x]/(x^5+2, x^4+x^3+x^2+x+1)$.

(a) Beweisen Sie, dass $3 \in (x^5+2, x^4+x^3+x^2+x+1)$ gilt.

(b) Zeigen Sie, dass K ein Körper ist.

(c) Beweisen Sie, dass K eine Galois-Erweiterung seines Primkörpers $\mathbb{F}_3$ ist, und bestimmen Sie die Galoisgruppe von $K|\mathbb{F}_3$.

(d) Sei α die Restklasse von x in K. Zeigen Sie, dass $\{1, \alpha, \alpha^2, \alpha^3\}$ eine $\mathbb{F}_3$-Basis von K ist, und bestimmen Sie die Darstellungsmatrizen der Elemente der Galoisgruppe $\mathrm{Gal}(K|\mathbb{F}_3)$ bezüglich dieser Basis.

Lösung:
zu (a) Setzen wir $I = (f, g)$ mit $f = x^5+2$ und $g = x^4+x^3+x^2+x+1$, dann ist auch $(x-1)g = x^5-1$ in I enthalten, und damit auch $3 = (x^5+2) - (x^5-1) = f + (1-x)g$.

zu (b) Wir beweisen zunächst mit Hilfe des Isomorphiesatzes für Ringe, dass $K = \mathbb{Z}[x]/I$ isomorph zu $\mathbb{F}_3[x]/(\bar{f})$ ist, wobei $\bar{f}$ das Bild von f in $\mathbb{F}_3[x]$ bezeichnet. Auf Grund der universellen Eigenschaft gibt es einen eindeutig bestimmten Ringhomomorphismus $\pi_1 : \mathbb{Z}[x] \to \mathbb{F}_3[x]$, $h \mapsto \bar{h}$ der den kanonischen Epimorphismus $\mathbb{Z} \to \mathbb{F}_3$ auf $\mathbb{Z}[x]$ fortsetzt und dabei $x \in \mathbb{Z}[x]$ auf $x \in \mathbb{F}_3[x]$ abbildet. Dabei entsteht das Polynom $\bar{h} \in \mathbb{F}_3[x]$ jeweils durch Anwendung des kanonischen Epimorphismus auf die Koeffizienten von h. Diese Abbildung ist surjektiv. Ist nämlich $\bar{h} = \sum_{i=0}^{m} \bar{a}_i x^i$ mit $m \in \mathbb{N}_0$ und $\bar{a}_0, ..., \bar{a}_m \in \mathbb{F}_3$ und ist $a_i \in \mathbb{Z}$ jeweils ein Urbild von $\bar{a}_i \in \mathbb{F}_3$ für $0 \le i \le m$, dann ist durch $h = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ offenbar ein Element mit $\pi_1(h) = \bar{h}$ gegeben.

Bezeichnen wir den kanonischen Epimorphismus $\mathbb{F}_3[x] \to \mathbb{F}_3[x]/(\bar{f})$ mit π_2, dann ist durch $\pi_2 \circ \pi_1$ ein Ringhomomorphismus $\mathbb{Z}[x] \to \mathbb{F}_3[x]/(\bar{f})$ gegeben. Als Komposition zweier surjektiver Abbildungen ist dieser ebenfalls surjektiv. Außerdem gilt $\ker(\pi_2 \circ \pi_1) = I$, denn für alle $h \in \mathbb{Z}[x]$ gilt die Äquivalenz

$$\begin{aligned} h \in \ker(\pi_2 \circ \pi_1) \quad &\Leftrightarrow \quad (\pi_2 \circ \pi_1)(h) = 0_{\mathbb{F}_3[x]/(\bar{g})} \quad \Leftrightarrow \quad \pi_2(\bar{h}) = \bar{0} + (\bar{g}) \quad \Leftrightarrow \quad \bar{h} + (\bar{g}) = \bar{0} + (\bar{g}) \\ &\Leftrightarrow \quad \bar{h} \in (\bar{g}) \quad \Leftrightarrow \quad \exists\, \bar{u} \in \mathbb{F}_3[x] : \bar{h} = \bar{u} \cdot \bar{g} \quad \Leftrightarrow \quad \exists\, u \in \mathbb{Z}[x] : h \equiv ug \bmod (3) \\ &\Leftrightarrow \quad \exists\, u, v \in \mathbb{Z}[x] : h = ug + 3v \quad \Leftrightarrow \quad \exists\, u, v \in \mathbb{Z}[x] : h = ug + v(f + (1-x)g) \\ &\Leftrightarrow \quad \exists\, u, v \in \mathbb{Z}[x] : h = vf + (u + (1-x)v)g \quad \Leftrightarrow \quad \exists\, u', v' \in \mathbb{Z}[x] : h = u'f + v'g \\ &\Leftrightarrow \quad h \in (f, g) \quad \Leftrightarrow \quad h \in I. \end{aligned}$$

(Im drittletzten Schritt erhält man die Richtung „$\Rightarrow$“ mit $u' = v$, $v' = u + (1-x)v$, und die Richtung „$\Leftarrow$“ mit $v = u'$, $u = v' - (1-x)u'$.) Auf Grund des Homomorphiesatzes für Ringe existiert also ein Isomorphismus $\bar{\phi} : K \to \mathbb{F}_3[x]/(\bar{f})$, gegeben durch $\bar{\phi}(h + I) = \bar{h} + (\bar{f})$ für alle $h \in \mathbb{Z}[x]$. Auf Grund der Isomorphie genügt es zu zeigen, dass $\mathbb{F}_3[x]/(\bar{f})$ ein Körper ist. Als Polynomring über einem Körper ist $\mathbb{F}_3[x]$ ein Hauptidealring. In einem solchen Ring sind die von irreduziblen Elementen erzeugte Hauptideale maximale Ideale. Ist $\bar{f}$ also irreduzibel, dann ist $(\bar{f})$ ein maximales Ideal in $\mathbb{F}_3[x]$, und daraus wiederum folgt, dass $\mathbb{F}_3[x]/(\bar{f})$ ein Körper ist.

Für den Nachweis der Irreduzibilität stellen wir zunächst fest, dass $\bar{f} \in \mathbb{F}_3[x]$ im Körper $\mathbb{F}_3$ keine Nullstelle besitzt, denn es ist $f(\bar{0}) = \bar{1} \neq \bar{0}$, $f(\bar{1}) = \bar{5} = \bar{2} \neq \bar{0}$ und $f(\bar{2}) = \overline{16} + \bar{8} + \bar{4} + \bar{2} + \bar{1} = \overline{31} = \bar{1} \neq \bar{0}$. Wäre $\bar{f}$ dennoch reduzibel, dann müsste $\bar{f}$ Produkt zweier irreduzibler Polynome $\bar{g}, \bar{h} \in \mathbb{F}_3[x]$ vom Grad 2 sein. Man kann durch direktes Nachrechnen überprüfen, dass keine Zerlegung von f der Form

$$x^4 + x^3 + x^2 + x + \bar{1} \quad = \quad (x^2 + ax + b)(x^2 + cx + d)$$

mit $a, b, c, d \in \mathbb{F}_3$ existiert. Wir wählen hier aber einen anderen Weg: Sei α eine Nullstelle von $\bar{g}$ in einem algebraischen Abschluss $\mathbb{F}_3^{\text{alg}}$ von $\mathbb{F}_3$. Weil $\bar{g}$ das Minimalpolynom von α über $\mathbb{F}_3$ ist, gilt $[\mathbb{F}_3(\alpha) : \mathbb{F}_3] = \text{grad}(\bar{g}) = 2$. Als zweidimensionaler $\mathbb{F}_3$-Vektorraum besteht $\mathbb{F}_3(\alpha)$ aus $3^2 = 9$ Elementen, stimmt also mit dem Zwischenkörper $\mathbb{F}_9$ von $\mathbb{F}_3^{\text{alg}}|\mathbb{F}_3$ überein. Wegen $\bar{f}(\bar{0}) \neq \bar{0}$ und $\bar{f} = \bar{g} \cdot \bar{h}$ gilt auch $\bar{g}(\bar{0}) \neq \bar{0}$. Daraus folgt $\alpha \in \mathbb{F}_9^\times$. Wegen $|\mathbb{F}_9^\times| = 9 - 1 = 8$ ist die Ordnung $\text{ord}(\alpha)$ von α in der multiplikativen Gruppe $\mathbb{F}_9^\times$ ein Teiler von 8. Andererseits ist α als Nullstelle von $\bar{f}$ auch eine Nullstelle von $x^5 - \bar{1} = (x - \bar{1})\bar{f}$. Es gilt also $\alpha^5 = \bar{1}$; wegen $\alpha \neq \bar{1}$ folgt daraus $\text{ord}(\alpha) = 5$. Weil aber 5 kein Teiler von 8 ist, hat unsere Annahme, das Polynom $\bar{f}$ sei reduzibel in $\mathbb{F}_3[x]$, zu einem Widerspruch geführt.

zu (c) Wie wir bereits in Teil (b) festgestellt haben, ist K isomorph zu $\mathbb{F}_3[x]/(\bar{f})$. Weil $\bar{f}$ ein irreduzibles Polynom vom Grad 4 ist, ist dieser Körper wiederum isomorph zu $\mathbb{F}_{81}$, dem eindeutig bestimmten Zwischenkörper von $\mathbb{F}_3^{\text{alg}}|\mathbb{F}_3$ mit $3^4 = 81$ Elementen. Für jedes $m \in \mathbb{N}$ gilt $[\mathbb{F}_{3^m} : \mathbb{F}_3] = m$, insbesondere also $[\mathbb{F}_{81} : \mathbb{F}_3] = 4$. Laut Vorlesung ist jede endliche Erweiterung $E|F$ bestehend aus endlichen Körpern E und F eine Galois-Erweiterung. Die Galoisgruppe $G = \text{Gal}(E|F)$ ist jeweils zyklisch von Ordnung $[E : F]$ und wird vom Frobenius-Automorphismus $\varphi_q : E \to E$, $\gamma \mapsto \gamma^q$ erzeugt, wobei $q = |F|$ ist. Insbesondere ist $\text{Gal}(K|\mathbb{F}_3) = \text{Gal}(\mathbb{F}_{81}|\mathbb{F}_3)$ also die vierelementige Gruppe $\langle \varphi_3 \rangle = \{\text{id}_K, \varphi_3, \varphi_3^2, \varphi_3^3\}$, mit $\varphi_3 : K \to K$, $\gamma \mapsto \gamma^3$.

zu (d) Die Darstellungmatrix der Abbildung id_V auf einem n-dimensionalen $\mathbb{F}_3$-Vektorraum V bezüglich einer beliebigen Basis ist immer die Einheitsmatrix $E_n \in \mathcal{M}_{n,\mathbb{F}_3}$. Somit ist E_4 die Darstellung von id_K. Für die Darstellungsmatrix von φ_3 bemerken wir zunächst, dass $\alpha = x + (\bar{f})$ laut Vorlesung eine Nullstelle von $\bar{f}$ ist und somit $\alpha^4 = -\bar{1} - \alpha - \alpha^2 - \alpha^3 = \bar{2} + \bar{2}\alpha + \bar{2}\alpha^2 + \bar{2}\alpha^3$ gilt. Wie wir bereits in Teil (b) festgestellt haben, ist $\alpha^5 = \bar{1}$ und somit $\alpha^6 = \alpha$. Damit erhalten wir $\varphi_3(\bar{1}) = \bar{1}$, $\varphi_3(\alpha) = \alpha^3 = \bar{0} + \bar{0} \cdot \alpha + \bar{0} \cdot \alpha^2 + \bar{1} \cdot \alpha^3$, $\varphi_3(\alpha^2) = \varphi_3(\alpha)^2 = (\alpha^3)^2 = \alpha^6 = \alpha = \bar{0} + \bar{1} \cdot \alpha + \bar{0} \cdot \alpha^2 + \bar{0} \cdot \alpha^3$ und $\varphi_3(\alpha^3) = \varphi_3(\alpha)^3 = (\alpha^3)^3 = \alpha^9 = \alpha^5 \cdot \alpha^4 = \alpha^4 = \bar{2} + \bar{2}\alpha + \bar{2}\alpha^2 + \bar{2}\alpha^3$. Jede dieser Gleichungen liefert eine Spalte der Darstellungsmatrix $A \in \mathcal{M}_{4,\mathbb{F}_3}$, insgesamt ist diese gegeben durch

$$A \quad = \quad \begin{pmatrix} \bar{1} & \bar{0} & \bar{0} & \bar{2} \\ \bar{0} & \bar{0} & \bar{1} & \bar{2} \\ \bar{0} & \bar{0} & \bar{0} & \bar{2} \\ \bar{0} & \bar{1} & \bar{0} & \bar{2} \end{pmatrix}.$$

Die Darstellungsmatrizen von φ_3^2 bzw. φ_3^3 sind gegeben durch

$$A^2 = \begin{pmatrix} \bar{1} & \bar{2} & \bar{0} & \bar{0} \\ \bar{0} & \bar{2} & \bar{0} & \bar{0} \\ \bar{0} & \bar{2} & \bar{0} & \bar{1} \\ \bar{0} & \bar{2} & \bar{1} & \bar{0} \end{pmatrix} \qquad \text{bzw.} \qquad A^3 = \begin{pmatrix} \bar{1} & \bar{0} & \bar{2} & \bar{0} \\ \bar{0} & \bar{0} & \bar{2} & \bar{1} \\ \bar{0} & \bar{1} & \bar{2} & \bar{0} \\ \bar{0} & \bar{0} & \bar{2} & \bar{0} \end{pmatrix}.$$

Aufgabe H22T3A5

Sei R ein kommutativer Ring mit Einselement, und sei I der Durchschnitt der maximalen Ideale von R.

(a) Zeigen Sie, dass I ein Ideal von R ist.

(b) Beweisen Sie, dass ein Element $a \in R$ genau dann in I liegt, wenn für alle $b \in R$ das Element $ab-1$ eine Einheit von R ist.

Lösung:
zu (a) Wir müssen überprüfen, dass $0_R \in I$ gilt, und dass mit $a, b \in I$ und $r \in R$ auch die Elemente $a+b$ und ra in I enthalten sind. Das Nullelement 0_R ist in jedem Ideal des Rings R enthalten, insbesondere in jedem maximalen Ideal, und damit auch im Durchschnitt I aller maximalen Ideale.

Die Elemente a und b sind in jedem maximalen Ideal $\mathfrak{m}$ von R enthalten (weil I der Durchschnitt aller maximalen Ideale ist). Weil $\mathfrak{m}$ ein Ideal ist, liege auch die Elemente $a+b$ und ra jeweils in $\mathfrak{m}$. Weil I der Durchschnitt aller maximalen Ideale $\mathfrak{m}$ von R ist, zeigt dies, dass $a+b$ und ra auch in I enthalten sind.

zu (b) Die Implikation „$\Rightarrow$“ beweisen wir durch Kontraposition. Sei $a \in R$, und nehmen wir an, dass $ab - 1_R$ für ein $b \in R$ keine Einheit von R ist. Zu zeigen ist, dass a dann nicht im Durchschnitt aller maximalen Ideale von R liegt. Aus $ab - 1_R \notin R^\times$ folgt, dass das Hauptideal $(ab - 1_R)$ nicht das Einheitsideal ist. Sei $\mathfrak{m}$ ein maximales Ideal mit $\mathfrak{m} \supseteq (ab-1_R)$ und nehmen wir an, dass a im Durchschnitt aller maximalen Ideale liegt. Dann gilt insbesondere $a \in \mathfrak{m}$, und damit auch $ab \in \mathfrak{m}$. Aus $ab - 1_R \in \mathfrak{m}$ folgt dann $1_R - ab \in \mathfrak{m}$ und $1_R = (1_R - ab) + ab \in \mathfrak{m}$. Aber dies ist unmöglich, denn da $\mathfrak{m}$ ein maximales Ideal von R ist, gilt $1_R \notin \mathfrak{m}$.

„$\Leftarrow$“ Nehmen wir an, dass $ab - 1_R$ für alle $b \in R$ eine Einheit ist, a aber nicht in I liegt. Dann existiert ein maximales Ideal $\mathfrak{m}$ mit $a \notin \mathfrak{m}$, und auf Grund der Maximalität von $\mathfrak{m}$ muss $(a) + \mathfrak{m} = (1_R)$ gelten. Insbesondere ist also das Einselement 1_R in $(a) + \mathfrak{m}$ enthalten. Es gibt also ein $b \in R$ und ein $m \in \mathfrak{m}$ mit $1_R = ab + m$. Auf Grund unserer Annahme ist $-m = ab - 1_R$ eine Einheit. Aber dies ist unmöglich, denn $-m$ liegt auch in $\mathfrak{m}$, und im maximalen Ideal $\mathfrak{m}$ sind keine Einheiten enthalten.