Thema Nr. 1
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1

Seien $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ die Gaußschen Zahlen und

$$N(a + bi) = a^2 + b^2$$

die übliche Norm. Für $\alpha, \beta \in \mathbb{Z}[i]$ ist α ein Teiler von β (Notation: $\alpha|\beta$), falls $\beta = \gamma \cdot \alpha$ für ein $\gamma \in \mathbb{Z}[i]$ gilt. Zeigen Sie:

(a) $4 + 5i$ ist ein Teiler von $14 - 3i$.

(b) $3 + 7i$ ist kein Teiler von $10 + 3i$.

(c) Für $\alpha = a + bi \in \mathbb{Z}[i]$ gilt: $N(\alpha)$ ist gerade $\Leftrightarrow 1 + i$ teilt α.

Aufgabe 2

Sei V ein K-Vektorraum und $f : V \to V$ eine K-lineare Abbildung. Es seien $m \geq 1$ und $a_0, \ldots, a_{m-1} \in K$ gegeben mit

$$f^m + a_{m-1}f^{m-1} + \cdots + a_1 f + a_0 = 0,$$

wobei m minimal gewählt ist (d.h. es gibt keine solche Relation mit kleinerem m). Zeigen Sie:

(a) Ist $a_0 = 0$, so ist f nicht invertierbar.

(b) Ist $a_0 \neq 0$, so ist f invertierbar.

Aufgabe 3

Sei $K \subset L$ eine algebraische Körpererweiterung. Es sei $\alpha \in L$ mit $K(\alpha) = L$. Zu jedem Zwischenkörper E ist P_E das Minimalpolynom von α über E.

(a) Zeigen Sie, dass $[L : E] = \deg(P_E)$ für jeden Zwischenkörper E gilt.

(b) Seien E und F zwei Zwischenkörper mit $F \subset E$. Zeigen Sie, dass P_E ein Teiler von P_F in $E[X]$ ist.

(c) Sei E ein Zwischenkörper. Sei F der Zwischenkörper erzeugt von den Koeffizienten von P_E. Zeigen Sie, dass $P_E = P_F$ gilt. Folgern Sie daraus, dass $E = F$ ist.

Fortsetzung nächste Seite!

Aufgabe 4

Gegeben sei die Gruppe der invertierbaren 3×3-Matrizen über dem Körper mit 2 Elementen

$$G = \mathrm{GL}_3(\mathbb{F}_2)\,.$$

(a) Verifizieren Sie, dass G die Ordnung 168 hat.

(b) Bestimmen Sie eine 2-Sylow-Gruppe von G.
Hinweis: Betrachten Sie Dreiecksmatrizen in G.

(c) Wie viele 2-Sylow-Gruppen hat G?
Hinweis: Betrachten Sie den Stabilisator einer 2-Sylow-Gruppe.

Aufgabe 5

Sei K ein Körper der Charakteristik 0 und $K(\alpha,\beta)/K$ eine endliche Galoiserweiterung. Seien weiter $K(\alpha)/K$ und $K(\beta)/K$ Galoiserweiterungen, sowie $K(\alpha) \cap K(\beta) = K$.
Setze $G = \mathrm{Gal}(K(\alpha,\beta)/K(\alpha+\beta))$. Zeigen Sie:

(a) Für $\sigma \in G$ gilt: $\sigma(\alpha) - \alpha = \beta - \sigma(\beta) \in K$.

(b) Es ist $K(\alpha+\beta) = K(\alpha,\beta)$.

Hinweis zu b): Berechnen Sie zunächst $\sigma^j(\alpha)$ unter Verwendung von (a).

Thema Nr. 2
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1

(a) Begründen Sie, dass die Permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 8 & 3 & 9 & 1 & 6 & 4 & 2 \end{pmatrix} \in S_9$$

in der alternierenden Gruppe A_9 liegt.

(b) Zeigen Sie, dass $\varphi(n)$ für $n \geq 3$ stets gerade ist – hierbei bezeichne φ die Eulersche φ-Funktion.

(c) Begründen Sie, dass in einem Integritätsbereich R aus $e^2 = e$, wobei $e \in R$, stets $e = 0$ oder $e = 1$ folgt.

(d) Bestimmen Sie den Körpergrad $[\mathbb{Q}(\sqrt[5]{7} \cdot e^{-2\pi i/5}) : \mathbb{Q}]$.

Aufgabe 2

Sei K ein Körper und K^K die Menge aller Abbildungen $K \to K$. Es sei die Abbildung

$$\varphi \colon K[X] \to K^K, \quad f \mapsto \varphi(f)$$

betrachtet, wobei $\varphi(f)(x) := f(x)$ für alle $x \in K$. Beweisen Sie:

(a) Genau dann ist φ injektiv, wenn K unendlich ist.

(b) Genau dann ist φ surjektiv, wenn K endlich ist.

Aufgabe 3

Sei R ein (nicht notwendig kommutativer) Ring mit Eins. Ein Element $x \in R$ heißt *nilpotent*, falls es ein $n \in \mathbb{N}$ mit $x^n = 0$ gibt.

(a) Zeigen Sie: Ist der Ring R kommutativ, und ist $u \in R$ eine Einheit sowie $x \in R$ nilpotent, so ist $u+x$ eine Einheit.

(b) Es sei R der Ring der 2×2-Matrizen über $\mathbb{Q}$. Geben Sie mit Begründung ein Beispiel für eine Einheit $u \in R$ und ein nilpotentes Element $x \in R$ derart, dass $u+x$ keine Einheit ist.

Fortsetzung nächste Seite!

Aufgabe 4

(a) Zeigen Sie, dass die Galoisgruppe einer galoisschen Körpererweiterung L/K vom Grad 143 stets zyklisch ist.

(b) Sei L/K eine galoissche Körpererweiterung vom Grad 55 mit nichtabelscher Galoisgruppe. Zeigen Sie: Es gibt genau einen echten Zwischenkörper M von L/K, sodass M/K eine Galoiserweiterung ist. Berechnen Sie den Grad $[M : K]$.

Aufgabe 5

(a) Sei K ein Körper, $n \geq 1$ eine natürliche Zahl und sei A eine beliebige $n \times n$-Matrix über K. Zeigen Sie: Es existiert eine endliche Körpererweiterung L/K derart, dass A einen Eigenwert $\lambda \in L$ besitzt.

(b) Begründen Sie, dass $L := \mathbb{Q}[T]/(T^3+T+1)$ ein Körper ist. Zeigen Sie, dass $\alpha := [T] \in L$ ein Eigenwert der linearen Abbildung

$$f\colon L^3 \to L^3\,, \quad f(u,v,w) := (-w, u-w, v)$$

ist, und geben Sie einen Eigenvektor zum Eigenwert α an.

Thema Nr. 3
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1

1. Zeigen Sie, dass durch
$$K = (\mathbf{Z}/7\mathbf{Z})[T]/(T^3 - 2)$$
ein Körper mit 343 Elementen gegeben wird.

2. Bestimmen Sie das Minimalpolynom der komplexen Zahl $z = \pi + \mathrm{e}i$ über $\mathbf{R}$.

3. Zeigen oder widerlegen Sie, dass das Polynom
$$f(X) = X^{2021} + 105\,X^{103} + 15\,X + 45$$
über folgenden Körpern K irreduzibel ist:

   (a) $K = \mathbf{Q}$,
   (b) $K = \mathbf{R}$,
   (c) $K = \mathbf{F}_2$,
   (d) $K = \mathbf{Q}[T]/(f(T))$
   (e) Begründen Sie, dass $\mathbf{Q}[T]/(f(T))$ ein Körper ist.

Aufgabe 2

1. Bestimmen Sie alle Nullstellen (mit Vielfachheiten) des Polynoms $f(X) := X^4 + 2$ über $\mathbf{F}_3$.

2. Berechnen Sie die galoissche Gruppe von $f(X)$ über $\mathbf{F}_3$.

3. Sei α eine Nullstelle von $g(X) := X^4 + 2$ in einem algebraischen Abschluss von $\mathbf{F}_5$. Zeigen Sie, dass dann auch 2α, 3α und 4α Nullstellen von $g(X)$ sind.

4. Zeigen Sie, dass das Polynom $g(X)$ über $\mathbf{F}_5$ irreduzibel ist.

5. Berechnen Sie die galoissche Gruppe von $g(X)$ über $\mathbf{F}_5$.

Fortsetzung nächste Seite!

Aufgabe 3

Seien G eine (endliche) Gruppe und $\varphi\colon G \to H$ ein surjektiver Gruppenhomomorphismus auf eine weitere Gruppe H.

1. Zeigen Sie, dass H auflösbar ist, wenn G auflösbar ist.
2. Zeigen Sie, dass H entweder trivial oder einfach ist, wenn G einfach ist.

Aufgabe 4

Sei R ein kommutativer Ring. Ein Element $a \in R$ heißt *nilpotent*, falls $a^n = 0$ für eine natürliche Zahl n.

1. Begründen Sie, warum in einem Körper das einzige nilpotente Element a das Element $a = 0$ ist.
2. Zeigen Sie, dass das *Nilradikal*

$$\mathfrak{n}\colon = \{a \in R \mid a \text{ ist nilpotent}\}$$

ein Ideal ist.

3. Zeigen Sie, dass das Nilradikal in jedem Primideal $\mathfrak{p}$ des Ringes R enthalten ist.
4. Berechnen Sie das Nilradikal des (endlichen) Ringes $\mathbf{Z}/\ell\mathbf{Z}$, wobei $\ell \geq 1$ eine natürliche Zahl ist.

Aufgabe 5

1. Geben Sie mit Begründung eine mögliche Abbildungsmatrix des Frobenius-Homomorphismus

$$F\colon \mathbf{F}_{25} \to \mathbf{F}_{25},$$

aufgefasst als Endomorphismus des $\mathbf{F}_5$-Vektorraumes $\mathbf{F}_{25}$, an.

2. Bestimmen Sie die Anzahl der Unterkörper, die der endliche Körper $\mathbf{F}_{81}$ besitzt.

Thema Nr. 1
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!
Alle Lösungsschritte sind sorgfältig zu begründen!

Aufgabe 1 (12 Punkte)

Sei R ein kommutativer Ring (mit 1).

(a) Geben Sie die Definition eines *größten gemeinsamen Teilers* zweier Elemente $a, b \in R$ an.

(b) Begründen Sie, dass in einem faktoriellen Ring je zwei Elemente einen größten gemeinsamen Teiler haben.

(c) Begründen Sie, dass je zwei Elemente des Polynomrings $\mathbb{Q}[x, y]$ einen größten gemeinsamen Teiler haben.

Zwei Elemente $a, b \in R$ heißen *teilerfremd*, wenn 1 ein größter gemeinsamer Teiler von a und b ist. Sie heißen *relativ prim*, wenn es $u, v \in R$ gibt mit $ua + vb = 1$.

(d) Zeigen Sie: Sind $a, b \in R$ relativ prim, dann sind sie auch teilerfremd.

(e) Geben Sie zwei Elemente $a, b \in \mathbb{Q}[x, y]$ an, die teilerfremd sind, aber nicht relativ prim.

Aufgabe 2 (12 Punkte)

Sei V ein unendlich-dimensionaler $\mathbb{R}$-Vektorraum, auf dem eine positiv definite symmetrische Bilinearform $\langle \cdot, \cdot \rangle$ definiert ist. Wir schreiben $\|v\| := \sqrt{\langle v, v \rangle}$ für $v \in V$.

Es seien $v_1, v_2, \ldots, v_n \in V$. Zeigen Sie: Der Schwerpunkt $s = \frac{1}{n}(v_1 + v_2 + \ldots + v_n)$ ist das eindeutig bestimmte Element $v \in V$, für das $\sum_{j=1}^{n} \|v - v_j\|^2$ minimal wird.

Hinweis: Schreiben Sie v als $v = s + w$.

Aufgabe 3 (12 Punkte)

Sei K ein Körper. Für Polynome $f, g \in K[x]$ sei $f \circ g$ das Polynom $f(g(x))$.

Beweisen Sie oder wiederlegen Sie durch ein Gegenbeispiel, ob folgende Aussagen für alle Körper K richtig sind.

(a) $\forall f, g \in K[x]\colon (f \text{ irreduzibel} \Longrightarrow f \circ g \text{ irreduzibel})$.

(b) $\forall f, g \in K[x]\colon (f \circ g \text{ irreduzibel} \Longrightarrow f \text{ irreduzibel})$.

(c) $\forall f, g \in K[x]\colon (f \circ g \text{ irreduzibel} \Longrightarrow g \text{ irreduzibel})$.

Fortsetzung nächste Seite!

Aufgabe 4 (12 Punkte)

(a) Wir betrachten die additiven Gruppen $\mathbb{Z} \subset \mathbb{Q}$.

Zeigen Sie: Die Faktorgruppe $\mathbb{Q}/\mathbb{Z}$ ist unendlich, aber jede endlich erzeugte Untergruppe von $\mathbb{Q}/\mathbb{Z}$ ist endlich.

(b) Sei $A = \{f : \mathbb{Z} \to \mathbb{Z}, x \mapsto ax + b \mid a = \pm 1, b \in \mathbb{Z}\}$.

Zeigen Sie: A ist eine Gruppe mit der Hintereinanderschaltung von Abbildungen als Verknüpfung, und diese Gruppe ist isomorph zum semidirekten Produkt der (additiven) Gruppe $\mathbb{Z}$ mit der (multiplikativen) Gruppe $\{\pm 1\}$, wobei $\{\pm 1\}$ auf $\mathbb{Z}$ durch Multiplikation operiert.

Aufgabe 5 (12 Punkte)

Sei $\mathbb{Q} \subset K \subset \mathbb{C}$, wobei K eine galoissche Körpererweiterung von $\mathbb{Q}$ vom Grad 2021 ist. Zeigen Sie:

(a) Es gibt Zwischenkörper $\mathbb{Q} \subset L_j \subset K$, $j \in \{1, 2\}$, mit $[L_1 : \mathbb{Q}] = 43$ und $[L_2 : \mathbb{Q}] = 47$, die über $\mathbb{Q}$ galoissch sind.

(b) Sei $\alpha \in K$, sodass $K = \mathbb{Q}(\alpha)$ gilt, und sei f das Minimalpolynom von α über $\mathbb{Q}$. Dann zerfällt f über $\mathbb{R}$ in Linearfaktoren.

Thema Nr. 2
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!
Alle Lösungsschritte sind sorgfältig zu begründen!

Aufgabe 1 (12 Punkte)

Sei G eine Gruppe und seien a, b, c Elemente aus G.

(a) Zeigen Sie, dass a und a^{-1} dieselbe Ordnung haben.

(b) Zeigen Sie, dass ab und ba dieselbe Ordnung besitzen.

(c) Zeigen Sie, dass abc und bca dieselbe Ordnung besitzen.

(d) Geben Sie Elemente a, b, c in der symmetrischen Gruppe S_3 an, so dass abc und bac nicht dieselbe Ordnung besitzen.

(e) Zeigen Sie, dass es in einer nicht kommutativen Gruppe G stets Elemente a, b, c gibt, so dass abc und bac nicht dieselbe Ordnung haben.

Aufgabe 2 (12 Punkte)

(a) Bestimmen Sie das Minimalpolynom m von $\sqrt[3]{2}$ über $\mathbb{Q}$. Zeigen Sie, dass m über $\mathbb{Q}[\sqrt[3]{2}]$ nicht in Linearfaktoren zerfällt.

(b) Sei $\mathbb{F}_5$ der endliche Körper mit fünf Elementen. Geben Sie einen Körperisomorphismus $\varphi\colon \mathbb{F}_5[\sqrt{2}] \to \mathbb{F}_5[\sqrt{3}]$ explizit an.

Aufgabe 3 (12 Punkte)

Es sei L/K eine Körpererweiterung vom Grad 2.

(a) Zeigen Sie, dass L/K stets normal ist.

(b) Zeigen Sie, dass L/K im Fall $\operatorname{char} K \neq 2$ stets separabel ist.

(c) Geben Sie (mit Begründung) jeweils ein Beispiel für eine separable und eine inseparable Körpererweiterung L/K vom Grad 2 im Fall $\operatorname{char} K = 2$ an.

Hinweis: für den zweiten Teil: Betrachten Sie den rationalen Funktionenkörper $k(T)$ über einem Körper k.

Fortsetzung nächste Seite!

Aufgabe 4 (12 Punkte)

Zu betrachten seien die Körpererweiterungen $\mathbb{Q}(\alpha)$ und $\mathbb{Q}(\beta)$ von $\mathbb{Q}$, wobei

$$\alpha := \sqrt{1+\sqrt{2}} \in \mathbb{R} \quad \text{und} \quad \beta := i\sqrt{\sqrt{2}-1} \in \mathbb{C}\,.$$

(a) Bestimmen Sie jeweils das Minimalpolynom von α und von β über $\mathbb{Q}$.

(b) Bestimmen Sie die Grade $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ und $[\mathbb{Q}(\beta) : \mathbb{Q}]$. Entscheiden Sie, ob die beiden Erweiterungen verschieden sind.

(c) Entscheiden und begründen Sie, ob die Körpererweiterungen $\mathbb{Q}(\alpha)$ und $\mathbb{Q}(\beta)$ von $\mathbb{Q}$ jeweils normal sind.

(d) Bestimmen Sie die Automorphismengruppen $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ und $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\beta))$.

Aufgabe 5 (12 Punkte)

(a) Sei G eine Gruppe und $\mathrm{Aut}(G)$ deren Automorphismengruppe. Zeigen Sie, dass folgende Abbildung wohldefiniert ist und einen Gruppenhomomorphismus darstellt:

$$c\colon G \to \mathrm{Aut(G)}\,, \quad g \mapsto [c_g\colon x \mapsto gxg^{-1}]\,.$$

(b) Bezeichne S_3 die symmetrische Gruppe des Grades 3. Beweisen Sie, dass die Automorphismengruppe $\mathrm{Aut}(S_3)$ zur Gruppe S_3 isomorph ist.

Thema Nr. 3
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!
Alle Lösungsschritte sind sorgfältig zu begründen!

Aufgabe 1 (12 Punkte)

Sei S_5 die symmetrische Gruppe auf $\{1,2,3,4,5\}$ und sei $A_5 \leq S_5$ die alternierende Gruppe. Zeigen Sie die folgenden Aussagen:

(a) Sei $U \leq S_5$ eine Untergruppe mit 3 oder 5 Elementen. Dann ist $U \leq A_5$.

(b) S_5 hat genau 10 Untergruppen der Ordnung 3.

(c) S_5 hat genau 6 Untergruppen der Ordnung 5.

Aufgabe 2 (12 Punkte)

Es sei p eine Primzahl und $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der endliche Körper mit p Elementen. Wir betrachten die Menge

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \;\middle|\; a \in \mathbb{F}_p^\times,\ b \in \mathbb{F}_p \right\}$$

von 2×2-Matrizen über dem Körper $\mathbb{F}_p$.

(a) Zeigen Sie, dass $G \subseteq \mathrm{GL}(2, \mathbb{F}_p)$ ist.

(b) Zeigen Sie, dass G eine Gruppe ist.

(c) Bestimmen Sie alle Primzahlen p, für die G abelsch ist.

(d) Bestimmen Sie alle Primzahlen p, für die G zu einer symmetrischen Gruppe S_n isomorph ist.

Aufgabe 3 (12 Punkte)

Sei L/K eine endliche Körpererweiterung und sei $\alpha \in L$. Zeigen Sie:

(a) Das Minimalpolynom f_α der K-linearen Abbildung $\varphi_\alpha \colon L \to L$, $x \mapsto \alpha x$, ist gleich dem Minimalpolynom g_α von α über K.

(b) Ist $L = K(\alpha)$, so stimmen das charakteristische und das Minimalpolynom von φ_α überein.

Fortsetzung nächste Seite!

Aufgabe 4 (12 Punkte)

Es sei $\mathbb{F}_2$ der Körper mit zwei Elementen und $f = X^4 + X + 1 \in \mathbb{F}_2[X]$.

(a) Zeigen Sie, dass f irreduzibel ist.

(b) Sei $K = \mathbb{F}_2[X]/(f) = \mathbb{F}_2(\alpha)$ mit $\alpha = \bar{X}$ die durch Adjunktion einer Nullstelle von f entstandene algebraische Körpererweiterung von $\mathbb{F}_2$.

Zeigen Sie, dass α ein Erzeuger der multiplikativen Gruppe $K^\times$ ist.

(c) Zeigen Sie: In $K[X]$ gilt

$$f = (X - \alpha) \cdot (X - \alpha^2) \cdot (X - \alpha^4) \cdot (X - \alpha^8)\,.$$

Aufgabe 5 (12 Punkte)

Seien m und n zwei positive ganze Zahlen mit $\mathrm{ggT}(m, n) = 1$. Für jede positive ganze Zahl a sei $\zeta_a = e^{2\pi i/a} \in \mathbb{C}$; ζ_a ist eine primitive a-te Einheitswurzel. Beweisen Sie die folgenden Aussagen:

(a) $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{mn})$.

(b) $[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] \cdot [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$.

(c) $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.

Thema Nr. 1
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!
Alle Lösungsschritte sind sorgfältig zu begründen!

Aufgabe 1 (12 Punkte)

Sei $A \in \mathrm{Mat}(2, \mathbb{Q})$ eine 2×2-Matrix mit rationalen Einträgen, sodass 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 geeignete Kreisteilungspolynome.

Aufgabe 2 (12 Punkte)

(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 $9, 99, 999, 9999, \ldots$ teilt.

Aufgabe 3 (12 Punkte)

Man betrachte die symmetrische Gruppe S_4 des Grades 4 und

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

(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 zur symmetrischen Gruppe 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.

Fortsetzung nächste Seite!

Aufgabe 4 (12 Punkte)

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

(b) Bestimmen Sie alle idempotenten Elemente des Rings $R := \mathbb{Z}/2022\mathbb{Z}$, d.h. alle Elemente $a \in R$ mit $a^2 = a$.

(c) Bestimmen Sie die Anzahl der Nullteiler im Ring $\mathbb{Z}/2022\mathbb{Z}$.

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

Aufgabe 5 (12 Punkte)

Für $n \in \mathbb{N}_+$ 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 Körpererweiterung von $\mathbb{Q}$.

Thema Nr. 2
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!
Alle Lösungsschritte sind sorgfältig zu begründen!

Aufgabe 1 (12 Punkte)

Gegeben sei die komplexe 2×2-Matrix

$$A = \begin{pmatrix} i & 2 \\ 0 & -i \end{pmatrix} \in \mathrm{Mat}(2, \mathbb{C}).$$

Berechnen Sie die Matrix A^{2022}.

Aufgabe 2 (12 Punkte)

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

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

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

Aufgabe 3 (12 Punkte)

Sei $n > 0$ eine natürliche Zahl 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 beide Eigenschaften für den von Ihnen angegebenen Ring erfüllt sind.
Tipp: Betrachten Sie $R = \mathbb{Q}[X, Y]/I$ für ein geeignetes Ideal I.

Fortsetzung nächste Seite!

Aufgabe 4 (12 Punkte)

Seien p eine Primzahl und $n > 0$ eine natürliche Zahl. 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.

Aufgabe 5 (12 Punkte)

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 $L = K_1 K_2$ 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 $L/\cancel{K}$ galoissch ist und bestimmen Sie die Galois-Gruppe $\mathrm{Gal}(L/\mathbb{Q})$ bis auf Isomorphie. $\mathbb{Q}$

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

Thema Nr. 3
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!
Alle Lösungsschritte sind sorgfältig zu begründen!

Aufgabe 1 (12 Punkte)

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

$$\varphi : G \xrightarrow{\sim} \mathrm{Bij}(\mathbb{F}_2^2 \setminus \{0\})$$

induziert. (Hier bezeichne $\mathrm{Bij}(M)$ die Gruppe der Bijektionen auf einer Menge 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.

Aufgabe 2 (12 Punkte)

(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 ganzzahlige Lösungen $(x, y) \in \mathbb{Z}^2$ der Gleichung $221\,x + 39\,y = 26$.

(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.

Aufgabe 3 (12 Punkte)

Es sei $R := \mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ der Ring der ganzen gaußschen 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 $(1 - i) \cap \mathbb{Z}$.

Fortsetzung nächste Seite!

Aufgabe 4 (12 Punkte)

Es sei K ein Teilkörper von $\mathbb{C}$, sodass $K/\mathbb{Q}$ eine Galoiserweiterung 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 $K/\mathbb{Q}(i)$.

Aufgabe 5 (12 Punkte)

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 $\mathbb{Q}$-Automorphismus $\varphi: K \longrightarrow \mathbb{C}$ mit $\varphi(\sqrt[3]{2}) = \sqrt{3}$ gibt.

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

Thema Nr. 1
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!
Alle Lösungsschritte sind sorgfältig zu begründen!

Aufgabe 1 (12 Punkte)

Gegeben sei die Gruppe

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathrm{Mat}(2, \mathbb{Q}) \mid a, b, c \in \mathbb{Q}, ac \neq 0 \right\}$$

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

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G \mid c = a \right\} \quad \text{und} \quad U = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G \mid b = 0 \right\}.$$

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

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

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.

Aufgabe 2 (12 Punkte)

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

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

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

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

Aufgabe 3 (12 Punkte)

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

(b) Beweisen Sie, dass $\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q}$ eine Galoiserweiterung ist und bestimmen Sie die Elemente der Galoisgruppe.

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

Aufgabe 4 (12 Punkte)

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

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

Aufgabe 5 (12 Punkte)

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

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

Thema Nr. 2
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!
Alle Lösungsschritte sind sorgfältig zu begründen!

Aufgabe 1 (12 Punkte)

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 $E \subset \mathbb{R}^3$ eine affine Ebene. Zeigen Sie, dass $C \cap E$ höchstens drei Elemente hat.

Aufgabe 2 (12 Punkte)

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

$$R = \{ \frac{a}{b} \mid a, b \in K[X],\ \mathrm{ggT}(a, b) = 1,\ b(0) \neq 0\} \subseteq L.$$

Zeigen Sie:

(a) Die Menge R ist ein Unterring 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.

Aufgabe 3 (12 Punkte)

(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 $x^n = 1$ 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 $R := \mathbb{Z}/2022\,\mathbb{Z}$ genau n Lösungen hat.

Aufgabe 4 (12 Punkte)

Sei $f = X^6 + 3 \in \mathbb{Q}[X]$, sei $\alpha \in \mathbb{C}$ eine Nullstelle von f, und sei $K = \mathbb{Q}(\alpha) \subset \mathbb{C}$. 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 Galoiserweiterung von $\mathbb{Q}$.

(d) Die Galoisgruppppe $\mathrm{Gal}(K/\mathbb{Q})$ ist nicht abelsch.

Aufgabe 5 (12 Punkte)

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 H vom Index 2 besitzt.

Thema Nr. 3
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!
Alle Lösungsschritte sind sorgfältig zu begründen!

Aufgabe 1 (12 Punkte)

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

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

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

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

Aufgabe 2 (12 Punkte)

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

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

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

Aufgabe 3 (12 Punkte)

Seien p, q, r Primzahlen mit $p < q < r$, und sei G eine Gruppe der Ordnung $p \cdot q \cdot r$. Für $i \in \{p, q, r\}$ bezeiche s_i die Anzahl der verschiedenen i-Sylowuntergruppen von G. Beweisen Sie:

(a) Besitzt G keine normale Sylowuntergruppe, so gilt $s_p \geq q$ und $s_q \geq r$ und $s_r = pq$.

(b) Die Gruppe G besitzt eine normale Sylowuntergruppe.

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

Aufgabe 4 (12 Punkte)

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 Galoiserweiterung seines Primkörpers $\mathbb{F}_3$ ist und bestimmen Sie die Galoisgruppe von $K/\mathbb{F}_3$.

(d) Sei x die Restklasse von X in K. Zeigen Sie, dass $\{x,\ x^3,\ x^9,\ x^{27}\}$ eine $\mathbb{F}_3$-Basis von K ist und bestimmen Sie die Darstellungsmatrizen der Elemente der Galoisgruppe $\mathrm{Gal}(K/\mathbb{F}_3)$ bzgl. dieser Basis.

Aufgabe 5 (12 Punkte)

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.

Thema Nr. 1
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!
Alle Lösungsschritte sind sorgfältig zu begründen!

Aufgabe 1 (12 Punkte)

(a) Es sei (A, ·) eine abelsche Gruppe. Zeigen Sie, dass die Abbildung

$$\phi\colon A \to A, \qquad a \mapsto a^{-1}$$

ein Gruppenhomomorphismus ist.

(b) Geben Sie ein Gegenbeispiel an, welches zeigt, dass die entsprechende Aussage für beliebige Gruppen im Allgemeinen falsch ist.

(c) Mit $\mathfrak{A}_4$ werde die alternierende Gruppe über vier Buchstaben bezeichnet. Bestimmen Sie diejenigen $n \in \mathbb{Z}_{\geq 0}$, für die es einen surjektiven Gruppenhomomorphismus $\phi\colon \mathfrak{A}_4 \to \mathbb{Z}/(n)$ gibt.

Aufgabe 2 (12 Punkte)

(a) Geben Sie die Definition von *Nullteilerfreiheit* eines kommutativen Rings an.

(b) Bestimmen Sie alle Nullteiler und Einheiten sowie die Inklusionen aller Ideale des kommutativen Rings $\mathbb{Z}/(27)$.

Aufgabe 3 (12 Punkte)

(a) Zeigen Sie, dass jeder irreduzible Faktor von $f := X^4 - 25 \in \mathbb{Q}[X]$ separabel über $\mathbb{Q}$ ist.

(b) Bestimmen Sie ein primitives Element eines Zerfällungskörpers L von f über $\mathbb{Q}$ und die Dimension von L über $\mathbb{Q}$.

(c) Berechnen Sie die Automorphismengruppe von L über $\mathbb{Q}$.

(d) Bestimmen Sie alle Zwischenkörper $\mathbb{Q} \subseteq K \subseteq L$ und ihre Inklusionen.

Aufgabe 4 (12 Punkte)

(a) Zeigen Sie, dass die Charakteristik eines endlichen Körpers eine Primzahl ist.

(b) Zeigen Sie, dass die Anzahl der Elemente eines endlich-dimensionalen Vektorraums V über einem endlichen Körper K eine Potenz der Charakteristik von K ist.

(c) Sei K ein endlicher Körper mit q Elementen; die Charakteristik von K sei ungleich 2. Berechnen Sie die Mächtigkeit der Bahn des Elementes

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(K)$$

unter der Operation von $\mathrm{GL}_2(K)$ durch Konjugation.

Aufgabe 5 (12 Punkte)

Seien K ein Körper und $f\colon V \to W$ eine lineare Abbildung zwischen endlich-dimensionalen K-Vektorräumen V und W. Seien

$$V^* := \mathrm{Hom}_K(V, K) \qquad \text{und} \qquad W^* := \mathrm{Hom}_K(W, K)$$

die Dualräume, sowie $f^*\colon W^* \to V^*$, $\varphi \mapsto \varphi \circ f$, die duale Abbildung.

(a) Sei $v_1, \ldots, v_n$ eine K-Basis von V. Zeigen Sie, dass f genau dann injektiv ist, wenn $f(v_1), \ldots, f(v_n)$ linear unabhängig sind.

(b) Zeigen Sie: Ist f injektiv, dann ist f^* surjektiv.

(c) Zeigen Sie: Ist f^* surjektiv, dann ist f injektiv.

Thema Nr. 2
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!
Alle Lösungsschritte sind sorgfältig zu begründen!

Aufgabe 1 (12 Punkte)

(a) Es seien $a, b \in \mathbb{Z}$. Zeigen Sie:

$$7 \mid (10a + b) \iff 7 \mid (a - 2b).$$

(b) Bestimmen Sie, für welche $r \in \mathbb{R}$ das folgende lineare Gleichungssystem (i) keine, (ii) genau eine, (iii) unendlich viele Lösungen hat.

$$\begin{aligned} rx + y + z &= 1 \\ x + ry + z &= 1 \\ x + y + rz &= 1 \end{aligned}$$

(c) Geben Sie ein externes direktes Produkt zyklischer Gruppen an, das isomorph ist zur Einheitengruppe $(\mathbb{Z}/40\mathbb{Z})^\times$.
(Hinweis: Hauptsatz über endliche abelsche Gruppen.)

(d) Bestimmen Sie eine Orthonormalbasis des $\mathbb{R}^3$ aus Eigenvektoren des Endomorphismus

$$\varphi\colon \mathbb{R}^3 \to \mathbb{R}^3, \quad \varphi\left(\begin{pmatrix} x \\ y \\ z \end{pmatrix}\right) = \begin{pmatrix} x - 2z \\ 0 \\ -2x + 4z \end{pmatrix}.$$

Aufgabe 2 (12 Punkte)

Es sei G eine Gruppe der Ordnung 30. Es bezeichnen U_3 und U_5 jeweils eine 3- und eine 5-Sylow-Gruppe von G. Zeigen Sie:

(a) Mindestens eine der Gruppen U_3 und U_5 ist ein Normalteiler von G.

(b) Ist U_3 normal, so hat G/U_3 eine Untergruppe vom Index 2. Ist U_5 normal, so hat G/U_5 eine Untergruppe vom Index 2.

(c) G hat eine Untergruppe U_{15} vom Index 2.

(d) Zeigen Sie, dass alle 3-Sylow-Gruppen und alle 5-Sylow-Gruppen von G in U_{15} enthalten sind.

(e) Folgern Sie, dass G genau eine 3-Sylow-Gruppe und genau eine 5-Sylow-Gruppe hat.

Aufgabe 3 (12 Punkte)

Es sei $R = \{x + y\sqrt{-31} \mid x, y \in \mathbb{Z}\} \subseteq \mathbb{C}$.

(a) Begründen Sie, dass R ein Ring ist.

(b) Zeigen Sie, dass R nicht faktoriell ist.
Hinweis: Beachten Sie $32 = (1 + \sqrt{-31})\,(1 - \sqrt{-31})$.

Aufgabe 4 (12 Punkte)

Seien p und q zwei Primzahlen. Bestimmen Sie den Zerfällungskörper des Polynoms $X^p - q \in K[X]$ für die Grundkörper $K = \mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$.

Aufgabe 5 (12 Punkte)

Es sei $\mathbb{F}_{625}$ der endliche Körper mit 625 Elementen mit Primkörper P. Bestimmen Sie die Anzahl der Elemente $a \in \mathbb{F}_{625}$ mit $P(a) = \mathbb{F}_{625}$.

Thema Nr. 3
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!
Alle Lösungsschritte sind sorgfältig zu begründen!

Aufgabe 1 (12 Punkte)

Es seien G die multiplikative Gruppe $(\mathbb{R}_{>0}, \cdot)$ und $X = \mathbb{R}^3$ der dreidimensionale $\mathbb{R}$-Vektorraum mit skalarer Multiplikation

$$\mathbb{R} \times X \to X\,, \quad (\lambda, x) \mapsto \lambda x\,.$$

Weiter sei die folgende Abbildung gegeben:

$$\cdot\colon G \times X \to X\,, \quad (g, x) \mapsto g \cdot x := gx$$

(das ist die skalare Multiplikation, eingeschränkt auf $G \times X$).

(a) Zeigen Sie, dass $\cdot$ eine Operation von G auf X ist.

(b) Bestimmen Sie die Menge F der Fixpunkte der Operation.

(c) Zeigen Sie, dass $R = \{x \in \mathbb{R}^3 \mid \|x\| = 1\} \cup \{0\}$ ein Repräsentantensystem der Bahnen der Operation ist.

Aufgabe 2 (12 Punkte)

Es seien $n \in \mathbb{Z}_{>0}$ und V der $\mathbb{R}$-Vektorraum $\mathbb{R}^{n \times n}$ der reellen $(n \times n)$-Matrizen. Für $A \in V$ sei $A^\top \in V$ die zu A transponierte Matrix. Weiter seien

$$U := \{A \in V \mid A^\top = A\} \qquad \text{und} \qquad W := \{A \in V \mid A^\top = -A\}\,.$$

Zeigen Sie:

(a) U und W sind Untervektorräume von V.

(b) $V = U \oplus W$.

Aufgabe 3 (12 Punkte)

Bestimmen Sie bis auf Isomorphie alle Gruppen der Ordnung $2023 = 7 \cdot 17^2$.

Aufgabe 4 (12 Punkte)

Es sei $\zeta \in \mathbb{C}$ eine primitive 7-te Einheitswurzel, und es seien $a := \zeta + \zeta^6$ und $b := \zeta + \zeta^2 + \zeta^4$.

(a) Geben Sie einen konkreten Isomorphismus zwischen der Einheitengruppe von $\mathbb{Z}/7\mathbb{Z}$ und der Galois-Gruppe von $\mathbb{Q}(\zeta)|\mathbb{Q}$ an.

(b) Zeigen Sie, dass die Körpererweiterungen $\mathbb{Q}(a)|\mathbb{Q}$ und $\mathbb{Q}(b)|\mathbb{Q}$ galoissch sind, und bestimmen Sie die zugehörigen Galois-Gruppen bis auf Isomorphie.

(c) Bestimmen Sie die Minimalpolynome von a und b über $\mathbb{Q}$.

Aufgabe 5 (12 Punkte)

Für einen kommutativen Ring R definieren wir $S(R) = \{r_1^2 + r_2^2 \mid r_1, r_2 \in R\}$.

(a) Zeigen Sie: Sind $r, r' \in S(R)$, dann gilt auch $rr' \in S(R)$.

(b) Bekanntlich sind die normierten irreduziblen Polynome in $\mathbb{R}[X]$ genau die Polynome der Form $X - r$ oder $(X-a)^2 + b^2$ mit $r, a \in \mathbb{R}$, $b \in \mathbb{R}_{>0}$.
Zeigen Sie: $S(\mathbb{R}[X]) = \{f \in \mathbb{R}[X] \mid \forall \xi \in \mathbb{R}\colon f(\xi) \geq 0\}$.

Prüfungsteilnehmer	Prüfungstermin	Einzelprüfungsnummer
Kennzahl: ______ Kennwort: ______ Arbeitsplatz-Nr.: ______	**Herbst 2023**	**63912**

Erste Staatsprüfung für ein Lehramt an öffentlichen Schulen

— Prüfungsaufgaben —

Fach: **Mathematik (vertieft studiert)**

Einzelprüfung: **Algebra**

Anzahl der gestellten Themen (Aufgaben): 3

Anzahl der Druckseiten dieser Vorlage: 7

Bitte wenden!

Thema Nr. 1
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1 (12 Punkte)

(a) Seien $n \geq 1$ eine natürliche Zahl und $p \neq 2$ eine Primzahl. Zeigen Sie:

$$p \mid (1 + 2 + 3 + \ldots + (n-1) + n) \iff p \mid n \text{ oder } p \mid (n+1).$$

(b) Bestimmen Sie die Anzahl der Elemente der Einheitengruppe

$$\left(\mathbb{Z}[X]/(2, X^3 + X^2 + X)\right)^*$$

des angegebenen Quotientenringes.

(c) Bestimmen Sie mithilfe des Chinesischen Restsatzes und unter vollständiger Angabe des Lösungsweges die kleinste natürliche Zahl $n \geq 1$, die die Kongruenzen $n \equiv 1 \pmod 3$, $n \equiv 2 \pmod 5$ und $n \equiv 0 \pmod 8$ erfüllt.

Aufgabe 2 (12 Punkte)

Im Folgenden sei S_n die symmetrische Gruppe.

(a) Sei $\sigma \in S_n$ ein Produkt $\sigma = \zeta_1 \cdots \zeta_m$ von paarweise disjunkten Zykeln ζ_j der Länge ℓ_j. Zeigen Sie, dass die Ordnung von σ gleich dem kleinsten gemeinsamen Vielfachen von $\ell_1, \ldots, \ell_m$ ist.

(b) Bestimmen Sie die maximale Ordnung eines Elements
(i) der S_6; (ii) der S_7.

Aufgabe 3 (12 Punkte)

(a) Seien G eine einfache Gruppe mit $|G| > 2$, die auf der endlichen Menge X operiere, und $\rho\colon G \to \Sigma(X) \simeq S_n$ $(n := |X|)$ der zugehörige Gruppenhomomorphismus in die symmetrische Gruppe von X. Zeigen Sie, dass $\rho(G)$ in der alternierenden Gruppe A_n enthalten ist.

(b) Seien G eine nicht-abelsche einfache Gruppe, $H \subseteq G$ eine Untergruppe sowie $n := (G : H) \geq 2$. Zeigen Sie, dass G isomorph zu einer Untergruppe von A_n ist, und dass $n \geq 5$ gilt.

(c) Zeigen Sie, dass keine endliche einfache Gruppe der Ordnung 80 existiert.

Aufgabe 4 (12 Punkte)

Sei R ein kommutativer Ring (mit 1). Sei weiter $I \subseteq R$ ein Ideal. Wir definieren das *Radikal* von I als

$$rad(I) = \{r \in R \mid r^n \in I \text{ für ein } n \in \mathbb{Z}_{>0}\}.$$

Zeigen Sie:

(a) $rad(I)$ ist ebenfalls ein Ideal von R.

(b) Ist I ein Primideal, dann gilt $rad(I) = I$.

Aufgabe 5 (12 Punkte)

(a) Zeigen Sie, dass der Kreisteilungskörper $\mathbb{Q}(\zeta_8)$ genau drei quadratische Teilkörper besitzt, d. h. Zwischenkörper $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\zeta_8)$ mit $[K : \mathbb{Q}] = 2$.

(b) Bestimmen Sie in Teil (a) drei Elemente $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}$ so, dass die Zwischenkörper $K_i := \mathbb{Q}(\sqrt{\alpha_i})$ $(1 \leq i \leq 3)$ genau die quadratischen Teilkörper sind.

(c) Zeigen Sie, dass das Polynom $X^4 + X + 1 \in \mathbb{F}_2[X]$ irreduzibel ist.

(d) Nach Teil (c) gilt $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$ für ein $\alpha \in \overline{\mathbb{F}}_2$ mit $\alpha^4 + \alpha + 1 = 0$. Bestimmen Sie die Grade $[\mathbb{F}_2(\beta) : \mathbb{F}_2]$ in den beiden Fällen $\beta = \alpha + 1$ und $\beta = \alpha^3 + 1$.

Thema Nr. 2
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1 (12 Punkte)

Sei $\omega \in \mathbb{C}$ eine primitive dritte Einheitswurzel.

(a) Zeigen Sie, dass $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$ eine Galois-Erweiterung ist.

(b) Bestimmen Sie den Grad $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}]$ dieser Erweiterung.

(c) Sei G die Menge der invertierbaren 2×2-Matrizen der Form $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ mit Einträgen in $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$. Zeigen Sie, dass G eine Untergruppe der Gruppe der invertierbaren 2×2-Matrizen ist, und geben Sie einen Isomorphismus $G \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ an.

Aufgabe 2 (12 Punkte)

(a) Geben Sie die Definition einer *auflösbaren Gruppe* an.

(b) Bestimmen Sie alle endlichen einfachen auflösbaren Gruppen.

Aufgabe 3 (12 Punkte)

(a) Seien G_1 und G_2 endliche Gruppen und $|G_1|$ teilerfremd zu $|G_2|$. Sei weiter $H \subseteq G_1 \times G_2$ eine Untergruppe. Zeigen Sie, dass es Untergruppen $H_1 \subseteq G_1$ und $H_2 \subseteq G_2$ gibt mit $H = H_1 \times H_2$.

(b) Geben Sie zwei Gruppen G_1 und G_2 an sowie eine Untergruppe $H \subseteq G_1 \times G_2$, sodass H nicht von der Form $H_1 \times H_2$ für zwei Untergruppen $H_1 \subseteq G_1$ und $H_2 \subseteq G_2$ ist.

(c) Sei G eine endliche Gruppe der Ordnung n mit folgenden Eigenschaften:

   (i) Für jeden Teiler $k > 0$ von n gibt es eine Untergruppe U von G der Ordnung k.

   (ii) G ist nicht abelsch.

   Zeigen Sie, dass G nicht einfach ist.

Aufgabe 4 (12 Punkte)

Es seien $x = (x_1, x_2, x_3, x_4)$, $y = (y_1, y_2, y_3, y_4)$, $z = (z_1, z_2, z_3, z_4) \in \mathbb{R}^4$ beliebig und

$$f\colon \mathbb{R}^4 \to \mathbb{R}\,, \quad (u_1, u_2, u_3, u_4) \mapsto \det \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \\ z_1 & z_2 & z_3 & z_4 \\ u_1 & u_2 & u_3 & u_4 \end{pmatrix}.$$

(a) Zeigen Sie, dass f eine lineare Abbildung ist.

(b) Zeigen Sie, dass x, y, z Elemente des Kerns von f sind.

(c) Zeigen Sie, dass der Kern von f genau dann der von x, y, z aufgespannte Unterraum ist, wenn diese Vektoren linear unabhängig sind.

(d) Bestimmen Sie den Kern von f im Fall, dass x, y, z linear abhängig sind.

Aufgabe 5 (12 Punkte)

Sei R ein kommutativer Ring mit 1.

(a) Sei $x \in R$ ein Element mit $x^m = 0$ für ein $m > 0$. Zeigen Sie, dass dann $1 + x \in R$ multiplikativ invertierbar ist.

(b) Sei $I \subseteq R$ ein Ideal. Zeigen Sie, dass dann auch

$$\sqrt{I} := \{x \in R \mid x^m \in I \text{ für ein } m > 0\}$$

ein Ideal in R ist.

(c) Zeigen Sie, dass $N(R) := \{x \in R \mid x^m = 0 \text{ für ein } m > 0\}$ ein Ideal in R ist.

(d) Geben Sie ein Beispiel für einen (nicht kommutativen) Ring R' an, in dem $N(R') \subseteq R'$ (wie in (c)) *kein* (Links-)Ideal ist.

Thema Nr. 3
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1 (12 Punkte)

Sei G eine Gruppe und H eine Untergruppe von G.

(a) Geben Sie die Definition des *Index* $(G : H)$ an. (G muss nicht endlich sein.)

(b) Zeigen Sie, dass $(G : H)$ ein Teiler von 168 ist, wenn H der Kern eines Homomorphismus $f\colon G \to \mathrm{GL}_3(\mathbb{F}_2)$ in die Gruppe der invertierbaren 3×3-Matrizen über dem Körper $\mathbb{F}_2$ ist.

Aufgabe 2 (12 Punkte)

Es seien $\alpha := \sqrt{\sqrt{12}+3} \in \mathbb{R}$, $\beta := i\sqrt{\sqrt{12}-3} \in \mathbb{C}$ und $L := \mathbb{Q}(\alpha, \beta) \subseteq \mathbb{C}$.

(a) Bestimmen Sie das Minimalpolynom $f = m_{\alpha,\mathbb{Q}}$ von α über $\mathbb{Q}$ und zeigen Sie, dass auch β eine Nullstelle von f ist.

(b) Begründen Sie, warum $L/\mathbb{Q}$ eine Galois-Erweiterung ist.

(c) Zeigen Sie, dass $L = \mathbb{Q}(\alpha, i)$ gilt, und bestimmen Sie den Grad $[L : \mathbb{Q}]$.

(d) Zeigen Sie, dass die Galois-Gruppe $\mathrm{Gal}(L/\mathbb{Q})$ einen Normalteiler der Ordnung 2 enthält.

Aufgabe 3 (12 Punkte)

Sei L Zerfällungskörper des Polynoms $f := X^4 - X^3 + 2X^2 - 2$ über $\mathbb{Q}$. Bestimmen Sie

(a) für eine Nullstelle $1 \neq \alpha \in L$ von f das Minimalpolynom von α über $\mathbb{Q}$,

(b) den Grad $[L : \mathbb{Q}]$.

Aufgabe 4 (12 Punkte)

(a) Seien p eine ungerade Primzahl und $n \geq 1$. Zeigen Sie, dass die Gleichung $x^2 = 1$ in $R = \mathbb{Z}/p^n\mathbb{Z}$ genau zwei Lösungen hat.

(b) Bestimmen Sie alle Lösungen der Gleichung $x^2 = 1$ im Ring $\mathbb{Z}/2023\mathbb{Z}$.
Hinweis: $2023 = 7 \cdot 17^2$.

Aufgabe 5 (12 Punkte)

Seien $R \neq 0$ ein kommutativer Ring und $F, G \in R[X]$ Polynome, wobei G als normiert angenommen sei. Dann (das sollen Sie nicht beweisen) existieren eindeutig bestimmte $A, B \in R[X]$ so, dass gelten $F = AG + B$ und $\deg(B) < \deg(G)$ (hierbei ist $\deg(0) := -\infty$). (Das ist Division mit Rest durch ein normiertes Polynom).

(a) Seien $f\colon R \to S \neq 0$ ein Ringhomomorphismus und $f[X]\colon R[X] \to S[X]$ der Ringhomomorphismus, der auf $R \subseteq R[X]$ mit f übereinstimmt und außerdem $f[X](X) = X$ erfüllt. Zeigen Sie, dass in $S[X]$ gilt $f[X](F) = f[X](A) \cdot f[X](G) + f[X](B)$, und dass diese Gleichung die Division mit Rest von $f[X](F)$ durch $f[X](G)$ ist.

(b) Zeigen Sie, dass genau ein Ideal $I \subseteq R$ existiert, sodass für jeden Ringhomomorphismus $f\colon R \to S \neq 0$ äquivalent sind:

(i) $f[X](G)$ teilt $f[X](F)$ in $S[X]$.

(ii) $f(I) = 0$.

(c) Bestimmen Sie das Ideal $I \subseteq R$ aus Teil (b) in den beiden folgenden Fällen:

(i) $R := \mathbb{Z}, \quad F := X^3 - 1, \quad G := X^2 + 1 \in R[X]$.

(ii) $R := \mathbb{Z}[Y], \quad F(X) := X^2 + Y, \quad G(X) := X - 1 \in R[X]$.