LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Dr. Ralf Gerkmann

Wintersemester 2024/25
15.02.2025

# Algebra und Zahlentheorie I

**(Lehramt Gymnasium, neue Studienordnung)**

## Klausur

Nachname: _____ Vorname: _____

Matrikelnr.: _____

Ihr Klausurergebnis können Sie auf der Vorlesungshomepage mit Hilfe eines Benutzernamens, eines Passworts und einer vierstelligen Identifikationsnummer abrufen, die Ihnen persönlich zugeordnet ist. Sie erhalten diese Daten während der Klausur.

| Aufgabe | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | $\sum$ |
|---|---|---|---|---|---|---|---|---|---|
| Punkte | | | | | | | | | |

*Hinweise:*

(a) Bitte überprüfen Sie, ob Sie **neun Blätter** (Deckblatt + 8 Aufgaben) erhalten haben.

(b) Für die Klausur sind **keine Hilfsmittel** (z.B. Skripten, handschriftliche Notizen, Taschenrechner) zugelassen.

(c) Schreiben Sie keine Lösungen zu unterschiedlichen Aufgaben auf dasselbe Blatt.

(d) Füllen Sie das Deckblatt bitte in Blockschrift aus. Schreiben Sie auf **jedes Blatt** Ihren **Vor- und Nachnamen**.

(e) Bitte denken Sie daran, jeden Schritt Ihrer Lösung zu begründen und explizit darauf hinzuweisen, wenn Sie Ergebnisse aus der Vorlesung verwenden. Die Verwendung von Ergebnissen aus Übungsaufgaben ist **nicht** zulässig.

(f) Bitte achten Sie darauf, dass Sie zu jeder Aufgabe nur eine Lösung abgeben; streichen Sie deutlich durch, was nicht gewertet werden soll.

(g) Bei Bedarf kann zusätzliches Schreibpapier angefordert werden. Bitte verwenden Sie keine eigenen Blätter.

Bearbeitungszeit: 120 Minuten

Viel Erfolg!

Name: _____

**Aufgabe 1.** (6+2+2 Punkte)

Sei $G$ eine zyklische Gruppe der Ordnung 36, $g \in G$ ein Element mit $G = \langle g \rangle$, und es seien $U, V$ die Untergruppen von $G$ definiert durch $U = \langle g^4 \rangle$ und $V = \langle g^9 \rangle$.

(a) Begründen Sie, dass $U$ und $V$ Normalteiler von $G$ sind, und bestimmen Sie die Ordnungen von $U$, $V$, $G/U$ und $G/V$.

(b) Bestimmen Sie die Ordnung des Elements $g^2U$ der Faktorgruppe $G/U$.

(c) Bestimmen Sie die Ordnung des Elements $g^7V$ der Faktorgruppe $G/V$.

Bitte begründen Sie jeweils Ihre Ergebnisse.

*Lösung:*

zu (a) Es gilt $\mathrm{ord}(g) = |\langle g \rangle| = |G| = 36$, und weil 4 und 9 Teiler von 36 sind, folgt $|U| = |\langle g^4 \rangle| = \mathrm{ord}(g^4) = \frac{36}{4} = 9$ und ebenso $|V| = \frac{36}{9} = 4$. Mit dem Satz von Lagrange erhalten wir $|G/U| = \frac{|G|}{|U|} = \frac{36}{9} = 4$ und $|G/V| = \frac{|G|}{|V|} = \frac{36}{4} = 9$.

zu (b) Die Elemente der Gruppe $G/U$ sind gegeben durch

$$G/U \quad = \quad \{hU \mid h \in U\} \quad = \quad \{g^m U \mid m \in \mathbb{Z}\} \quad = \quad \{(gU)^m \mid m \in \mathbb{Z}\}.$$

Die Gruppe $G/U$ ist also ebenfalls zyklisch, und $gU$ ist ein erzeugendes Element, mit Ordnung $\mathrm{ord}(gU) = |G/U| = 4$. Weil 2 ein Teiler von 4 ist, ist $g^2U = (gU)^2$ ein Element der Ordnung $\frac{4}{2} = 2$.

zu (c) Ebenso wie $G$ und $G/U$ ist auch $G/V$ zyklisch, und eine Rechung wie in Teil (b) zeigt, dass $gV$ ein erzeugendes Element ist, von Ordnung $\mathrm{ord}(gV) = |G/V| = 9$. Wegen $\mathrm{ggT}(7, 9) = 1$ ist $g^7V = (gV)^7$ ebenfalls ein Element der Ordnung 9.

Name: _____

**Aufgabe 2.** (2+3+5 Punkte)

Sei $G$ eine abelsche Gruppe, und sei $\phi : G \times G \to G$ die Abbildung definiert durch $\phi(g, h) = g^{-1}h$ für alle $(g, h) \in G \times G$.

(a) Zeigen Sie, dass $\phi$ ein Gruppenhomomorphismus ist.

(b) Weisen Sie nach, dass $\phi$ surjektiv ist.

(c) Sei $D = \{(g, g) \mid g \in G\}$. Zeigen Sie, dass $D$ ein Normalteiler von $G \times G$ ist, und dass ein Isomorphismus $(G \times G)/D \cong G$ von Gruppen existiert.

*Lösung:*

zu (a) Für alle $(g_1, h_1), (g_2, h_2) \in G \times G$ gilt

$$\phi((g_1, h_1) \cdot (g_2, h_2)) \quad = \quad \phi(g_1 g_2, h_1 h_2) \quad = \quad (g_1 g_2)^{-1}(h_1 h_2) \quad =$$
$$g_2^{-1} g_1^{-1} h_1 h_2 \quad = \quad g_1^{-1} h_1 g_2^{-1} h_2 \quad = \quad \phi(g_1, h_1) \cdot \phi(g_2, h_2).$$

zu (b) Sei $h \in G$ vorgegeben. Dann gilt $\phi(e, h) = e^{-1}h = eh = h$, wobei $e$ das Neutralelement von $G$ bezeichnet. (Bei diesem Aufgabenteil war ein häufiger Fehler, dass nicht von einem beliebigen Element $h \in G$, sondern von einem Element der Form $g^{-1}h$ ausgegangen wurde, mit $g, h \in G$. Damit beweist man aber nur die Surjektivität von $\phi$ als Abbildung $G \to \mathrm{im}(\phi)$, die offensichtlich auch für jede andere Abbildung erfüllt ist.)

zu (c) In den Aufgabenteilen (a) und (b) gezeigt wurde, dass $\phi$ ein surjektiver Gruppenhomomorphismus ist. Wenn außerdem $D = \ker(\phi)$ gilt, dann erhält man durch Anwendung des Homomorphiesatzes für Gruppen einen Isomorphismus der angegebenen Form. Außerdem ist $D$ dann ein Normalteiler von $G$, da Kerne von Gruppenhomomorphismen laut Vorlesung stets Normalteiler sind.

Für den Nachweis der Gleichung $D = \ker(\phi)$ sei $(g, h) \in G \times G$ vorgegeben. Dann gilt die Äquivalenz

$$(g, h) \in \ker(\phi) \quad \Leftrightarrow \quad \phi(g, h) = e \quad \Leftrightarrow \quad g^{-1}h = e \quad \Leftrightarrow \quad g = h \quad \Leftrightarrow \quad (g, h) = (g, g) \quad \Leftrightarrow \quad (g, h) \in D.$$

Name: _____

**Aufgabe 3.** (4+3+3 Punkte)

(a) Geben Sie ein $r \in \mathbb{N}$ und Gruppen $G_1, ..., G_r$ an, so dass jede abelsche Gruppe der Ordnung 36 zu genau einer dieser Gruppen $G_j$ mit $1 \leq j \leq r$ isomorph ist. Ein Nachweis ist hier *nicht* erforderlich.

(b) Begründen Sie, dass die Gruppe $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ nicht zu $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ isomorph ist.

(c) Wie in der Vorlesung bezeichnet $S_n$ für jedes $n \in \mathbb{N}$ die symmetrische Gruppe mit der Ordnung $n!$, und für jedes $n \in \mathbb{N}$ mit $n \geq 3$ sei $D_n$ die $2n$-elementige Diedergruppe. Zeigen Sie, dass $S_3 \times S_3$ und $D_9 \times \mathbb{Z}/2\mathbb{Z}$ nicht abelsche, nicht zueinander isomorphe Gruppen der Ordnung 36 sind.

*Lösung:*

zu (a) Die Zahl $r = 4$ und die Gruppen $G_1 = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$, $G_2 = (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/9\mathbb{Z}$, $G_3 = \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2$, $G_4 = (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z})^2$ haben die angegebene Eigenschaft. (Alternativ hätte man auch $G_1 = \mathbb{Z}/36\mathbb{Z}$, $G_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$, $G_3 = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ und $G_4 = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ angeben können.)

zu (b) Für alle $(a, b) \in \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ gilt $6 \cdot (a, b) = (6 \cdot a, 6 \cdot b) = (\bar{0}, \bar{0})$. Die Ordnung jedes Elements in $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ ist also ein Teiler von 6. Wäre die Gruppe zu $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ isomorph, dann hätte auch jedes Element in $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ diese Eigenschaft, beispielsweise auch das Element $(\bar{1}, \bar{0})$. Es wäre also $(6 \cdot \bar{1}, \bar{0}) = 6 \cdot (\bar{1}, \bar{0}) = (\bar{0}, \bar{0})$ und somit $6 \cdot \bar{1} = \bar{0}$ in $\mathbb{Z}/4\mathbb{Z}$. Tatsächlich gilt in $\mathbb{Z}/4\mathbb{Z}$ aber $6 \cdot \bar{1} = \bar{6} = \bar{2} \neq \bar{0}$.

zu (c) Aus der Vorlesung ist bekannt, dass $S_3$ nicht abelsch ist (da z.B. $(1\ 2) \circ (1\ 3) \neq (1\ 3) \circ (1\ 2)$ gilt), und ebenso $D_n$ für alle $n \geq 3$, insbesondere $D_9$. Daraus folgt, dass auch $S_3 \times S_3$ und $D_9 \times \mathbb{Z}/2\mathbb{Z}$ nicht abelsch sind. Es gilt $|S_3 \times S_3| = |S_3| \cdot |S_3| = 6 \cdot 6 = 36$, und aus $|D_n| = 2n$ für alle $n \geq 3$ folgt $|D_9 \times \mathbb{Z}/2\mathbb{Z}| = |D_9| \cdot |\mathbb{Z}/2\mathbb{Z}| = 18 \cdot 2 = 36$.

Wegen $|S_3| = 6$ gilt $(\sigma, \tau)^6 = (\sigma^6, \tau^6) = (\mathrm{id}, \mathrm{id})$ für alle $(\sigma, \tau) \in S_3 \times S_3$. Die Ordnung jedes Elements in $S_3 \times S_3$ ist also ein Teiler von 6. Wäre die Gruppe zu $D_9 \times \mathbb{Z}/2\mathbb{Z}$ isomorph, dann würde dasselbe für die Elemente von $D_9 \times \mathbb{Z}/2\mathbb{Z}$ gelten. Es wäre also $(\rho^6, 6 \cdot a) = (\rho, a)^6 = e_{D_9 \times \mathbb{Z}/2\mathbb{Z}} = (e_{D_9}, \mathbb{Z}/0\mathbb{Z})$ für alle $(\rho, a) \in D_9 \times \mathbb{Z}/2\mathbb{Z}$.

Insbesondere wäre also $\rho^6 = e_{D_9}$ für alle $\rho \in D_9$, d.h. auch die Ordnung jedes Elements in $D_9$ wäre ein Teiler von 6. Aber aus der Vorlesung ist bekannt, dass $D_n$ für alle $n \geq 3$ jeweils ein Element der Ordnung $n$ enthält, also $D_9$ ein Element der Ordnung 9, und 9 ist kein Teiler von 6.

Name: _____

**Aufgabe 4.** (4+3+3 Punkte)

Sei $G$ eine Gruppe der Ordnung 2028. (Es ist $2028 = 2^2 \cdot 3 \cdot 13^2$.)

(a) Beweisen Sie mit Hilfe der Sylowsätze, dass $G$ einen abelschen Normalteiler $N$ der Ordnung 169 besitzt.

(b) Zeigen Sie: Besitzt die Faktorgruppe $G/N$ einen Normalteiler der Ordnung 3 oder 4, dann ist $G$ auflösbar.

(c) Setzen wir nun voraus, dass $G/N$ keinen Normalteiler der Ordnung 3 besitzt. Zeigen Sie, dass es in $G/N$ dann genau 8 Elemente der Ordnung 3 gibt.

*Lösung:*

zu (a) Es sei $\nu$ die Anzahl der 13-Sylowgruppen von $G$. Auf Grund des Dritten Sylowsatzes ist $\nu$ ein Teiler von $2^2 \cdot 3 = 12$, also insbesondere $\nu \leq 12$, außerdem $\nu \equiv 1 \bmod 13$, also $13 \mid (\nu - 1)$. Im Fall $\nu - 1 \neq 0$ wäre $\nu - 1 \geq 13$, wegen $\nu - 1 \leq 11 < 13$ folgt aber $\nu - 1 = 0$ und $\nu = 1$. (Man kann natürlich wie gewohnt auch die sechs Teiler von 12 hinschreiben und feststellen, dass diese alle nicht kongruent zu 1 modulo 13 sind.)

Sei $N$ die einzige 13-Sylowgruppe von $G$. Wegen $\nu = 1$ folgt aus dem Zweiten Sylowsatz, dass $N$ ein Normalteiler von $G$ ist. Wegen $|G| = 2^2 \cdot 3 \cdot 13^2$ gilt $|N| = 13^2 = 169$. Als Gruppe von Primzahlquadratordnung in $N$ abelsch.

zu (b) Nach dem Satz von Lagrange gilt $|G/N| = (G : N) = \frac{|G|}{|N|} = \frac{2028}{169} = 12$. Sei $\bar{M}$ ein Normalteiler von $\bar{G} = G/N$ der Ordnung 3 oder 4. Dann ist $\bar{G}/\bar{M}$ (wiederum nach dem Satz von Lagrange) von Ordnung $\frac{12}{|\bar{M}|}$, also von Ordnung 4 oder 3. Laut Vorlesung ist jede Gruppe von Primzahlordnung zyklisch, und somit auch abelsch, und jede Gruppe von Primzahlquadratordnung ist abelsch. Da 3 eine Primzahl und 4 ein Primzahlquadrat ist, sind $\bar{M}$ und $\bar{G}/\bar{M}$ abelsche Gruppen, damit auch auflösbar. Aus der Auflösbarkeit von $\bar{M}$ und $\bar{G}/\bar{M}$ folgt laut Vorlesung die Auflösbarkeit von $\bar{G}$.

zu (c) Sei $\bar{\nu}_3$ die Anzahl der 3-Sylowgruppen von $\bar{G}$; dies sind genau die Untergruppen von $\bar{G}$ der Ordnung 4. Wegen $|\bar{G}| = 12 = 3 \cdot 4$ und dem Dritten Sylowsatz folgt $\bar{\nu}_3 \mid 4$, $\bar{\nu}_3 \in \{1, 2, 4\}$, und außerdem $\bar{\nu}_3 \equiv 1 \bmod 3$. Wegen $2 \not\equiv 1 \bmod 3$ folgt $\bar{\nu}_3 \in \{1, 4\}$. Im Fall $\bar{\nu}_3 = 1$ gäbe es in $\bar{G}$ nur eine 3-Sylowgruppe (von Ordnung 3), und nach dem Zweiten Sylowsatz wäre dies ein Normalteiler, was aber laut Voraussetzung ausgeschlossen ist. Also muss $\bar{\nu}_3 = 4$ gelten.

Es gibt in $\bar{G}$ also genau vier Untergruppen der Ordnung 3. Da 3 eine Primzahl ist, sind diese zyklisch und enthalten jeweils genau $\varphi(3) = 2$ Elemente der Ordnung 3. Andererseits ist jedes Element $\bar{g} \in \bar{G}$ in genau einer solchen Untergruppe enthalten (nämlich in $\langle \bar{g} \rangle$). Daraus folgt, dass die Anzahl der Elemente der Ordnung 3 in $G$ gleich $2\bar{\nu}_3 = 2 \cdot 4 = 8$ ist.

Name: _____

**Aufgabe 5.** (4+4+2 Punkte)

Sei $R = \left\{ \frac{a}{15^n} \mid a \in \mathbb{Z} \ , \ n \in \mathbb{N}_0 \right\}$.

(a) Überprüfen Sie, dass $R$ ein Teilring von $\mathbb{R}$ ist.

(b) Zeigen Sie, dass $R = \mathbb{Z}[\frac{1}{3}, \frac{1}{5}]$ gilt.

(c) Begründen Sie, dass $R$ unendlich viele Einheiten besitzt.

*Lösung:*

zu (a) Die Gleichung $1 = \frac{1}{15^0}$ zeigt (wegen $1 \in \mathbb{Z}$ und $0 \in \mathbb{N}_0$), dass das Einselement 1 von $\mathbb{R}$ in $R$ enthalten ist. Seien nun $\alpha, \beta \in R$ vorgegeben. Zu zeigen ist $\alpha - \beta \in R$ und $\alpha\beta \in R$. Wegen $\alpha, \beta \in R$ gibt es $a, b \in \mathbb{Z}$ und $m, n \in \mathbb{N}_0$ mit $\alpha = \frac{a}{15^m}$ und $\beta = \frac{b}{15^n}$. Wegen

$$\alpha - \beta \quad = \quad \frac{a}{15^m} - \frac{b}{15^n} \quad = \quad \frac{15^n a - 15^m b}{15^{m+n}}$$

und $15^n a - 15^m b \in \mathbb{Z}$, $m + n \in \mathbb{N}_0$ gilt $\alpha - \beta \in R$, und aus $\alpha\beta = \frac{ab}{15^{m+n}}$, $ab \in \mathbb{Z}$ und $m + n \in \mathbb{N}_0$ folgt $\alpha\beta \in R$.

zu (b) Da $R$ nach Teil (a) ein Teilring von $\mathbb{R}$ ist, genügt es laut Vorlesung zu zeigen, dass $\mathbb{Z} \cup \{\frac{1}{3}, \frac{1}{5}\} \subseteq R$ gilt, und dass für jeden Teilring $S$ von $\mathbb{R}$ mit $\mathbb{Z} \cup \{\frac{1}{3}, \frac{1}{5}\} \subseteq S$ jeweils auch $R \subseteq S$ gilt. Für jedes $a \in \mathbb{Z}$ zeigt die Gleichung $a = \frac{a}{15^0}$, dass $a$ in $R$ enthalten ist. Wegen $\frac{1}{3} = \frac{5}{15^1}$ gilt $\frac{1}{3} \in R$, und wegen $\frac{1}{5} = \frac{3}{15^1}$ ist auch $\frac{1}{5}$ in $R$ enthalten.

Sei nun $S$ ein beliebiger Teilring von $\mathbb{R}$ mit $\mathbb{Z} \cup \{\frac{1}{3}, \frac{1}{5}\} \subseteq S$ und $\alpha \in R$. Zu zeigen ist $\alpha \in S$. Wegen $\alpha \in R$ gibt es ein $a \in \mathbb{Z}$ und ein $m \in \mathbb{N}_0$ mit $\alpha = \frac{a}{15^m}$. Aus $\frac{1}{3}, \frac{1}{5} \in S$ folgt $\frac{1}{15} = \frac{1}{3} \cdot \frac{1}{5} \in S$ und damit auch $\frac{1}{15^m} = (\frac{1}{15})^m \in S$. Aus $a \in \mathbb{Z}$ folgt $a \in S$, und damit wiederum erhalten wir $\alpha = a \cdot \frac{1}{15^m} \in S$.

zu (c) Wegen $\mathbb{Z} \subseteq R$ gilt für jedes $m \in \mathbb{N}_0$ jeweils $15^m \in R$, andererseits aber auch $15^{-m} = \frac{1}{15^m} \in R$. Wegen $15^m \cdot 15^{-m} = 1$ zeigt dies, dass $15^m \in R$ für jedes $m \in \mathbb{N}_0$ eine Einheit in $R$ ist. Dies zeigt, dass $R$ unendlich viele Einheiten besitzt. (Es handelt sich um lauter verschiedene Elemente von $R$, denn für alle $m, n \in \mathbb{N}_0$ folgt aus $m < n$ jeweils $15^m < 15^n$, insbesondere also $15^m \neq 15^n$.)

Name: _____

**Aufgabe 6.** (7+3 Punkte)

Sei $R = \mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$, und es sei $N : R \to \mathbb{N}_0$ die Normfunktion gegeben durch $N(a+b\sqrt{-2}) = a^2+2b^2$ für alle $a, b \in \mathbb{N}_0$. Ohne Beweis darf verwendet werden, dass $R$ ein euklidischer Ring ist, mit $N|_{R\setminus\{0\}}$ als Höhenfunktion.

(a) Untersuchen Sie, welche der folgenden Zahlen Primelemente im Ring $R$ sind:
$1 + \sqrt{-2}$, 5, 6 und 11

(b) Entscheiden Sie, ob das Hauptideal (5) in $R$ ein Primideal bzw. sogar ein maximales Ideal ist, und begründen Sie Ihre Entscheidung jeweils mit Hilfe geeigneter Sätze aus der Vorlesung.

*Lösung:*

zu (a) Als euklidischer Ring ist $R$ insbesondere ein Hauptidealring. Daraus folgt, dass die Primelemente in $R$ genau die irreduziblen Elemente sind. Es ist $N(1 + \sqrt{-2}) = 1^2 + 2 \cdot 1^2 = 3$ eine Primzahl. Daraus folgt laut Vorlesung, dass $1 + \sqrt{-2}$ irreduzibel und somit prim ist.

Es ist $N(5) = 5^2$ ein Primzahlquadrat, und die Gleichung $a^2 + 2b^2 = 5$ ist mit $a, b \in \mathbb{Z}$ nicht lösbar. (Es müsste $|b| \leq 1$ gelten, und weder 5 noch $5 - 2 \cdot 1^2 = 3$ ist ein Quadrat in $\mathbb{Z}$.) Daraus folgt, dass auch 5 in $R$ irreduzibel und prim ist. Wegen $N(2) = 4 > 1$ und $N(3) = 9 > 1$ ist $6 = 2 \cdot 3$ eine Zerlegung von 6 in Nicht-Einheiten des Rings $R$. Also ist 6 in $R$ reduzibel, und damit nicht prim. Ebenso ist $11 = (3 + \sqrt{-2})(3 - \sqrt{-2})$ wegen $N(3 \pm \sqrt{-2}) = 3^2 + 2 \cdot 1^2 = 9 + 2 = 11 > 1$ eine Zerlegung in Nicht-Einheiten, und somit auch 11 in $R$ kein Primelement.

zu (b) Wie bereits (a) festgestellt, ist 5 ein Primelement, und für jedes Primelement $p$ in einem Integritätsbereich ist das Hauptideal $(p)$ ein Primideal. Also ist (5) in $R$ ein Primideal. Darüber hinaus ist $R$ ein Hauptidealring, und laut Vorlesung sind in einem Hauptidealring die Primideale ungleich (0) genau die maximalen Ideale. Also ist (5) auch ein maximales Ideal.

Name: _____

**Aufgabe 7.** (4+4+2 Punkte)

Aus Aufgabe 4 ist bereits bekannt, dass die Zahl 2028 die Primfaktorzerlegung $2028 = 2^2 \cdot 3 \cdot 13^2$ besitzt.

(a) Zeigen Sie mit Hilfe geeigneter Sätze, dass die prime Restklassengruppe $(\mathbb{Z}/2028\mathbb{Z})^\times$ zu $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$ isomorph ist.

(b) Zeigen Sie, dass $(\mathbb{Z}/2028\mathbb{Z})^\times$ ein Element der Ordnung 156 besitzt, und dass es in $(\mathbb{Z}/2028\mathbb{Z})^\times$ keine Elemente größerer Ordnung gibt.

(c) Bestimmen Sie die Anzahl der Elemente der Ordnung 2 und die Anzahl der Elemente der Ordnung 13 in $(\mathbb{Z}/2028\mathbb{Z})^\times$. Hier ist *kein* Nachweis erforderlich.

*Lösung:*
zu (a) Weil $2028 = 2^2 \cdot 3 \cdot 13^2$ eine Zerlegung von 2028 in paarweise teilerfremde Faktoren ist, existiert auf Grund des Chinesischen Restsatzes ein Isomorphismus

$$(\mathbb{Z}/2028\mathbb{Z})^\times \quad \cong \quad (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/13^2\mathbb{Z})^\times.$$

Laut Vorlesung gilt $(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$ und (weil 3 eine Primzahl ist) auch $(\mathbb{Z}/3\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$. Weil $13^2$ eine ungerade Primzahlpotenz ist, ist $(\mathbb{Z}/13^2\mathbb{Z})^\times$ eine zyklische Gruppe, von Ordnung $\varphi(13^2) = 13 \cdot 12 = 3 \cdot 4 \cdot 13$, und somit

$$(\mathbb{Z}/13^2\mathbb{Z})^\times \quad \cong \quad \mathbb{Z}/3 \cdot 4 \cdot 13\mathbb{Z} \quad \cong \quad \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}.$$

Insgesamt erhalten wir

$$(\mathbb{Z}/2028\mathbb{Z})^\times \quad \cong \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}) \quad \cong \quad (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}.$$

zu (b) Weil $156 = 3 \cdot 4 \cdot 13$ ein gemeinsames Vielfaches von 2, 3, 4 und 13 ist, gilt $156 \cdot (a, b, c, d, e) = (\bar{0}, \bar{0}, \bar{0}, \bar{0}, \bar{0})$ für alle Elemente $(a, b, c, d, e)$ aus $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$. Also ist die Ordnung jedes Elements der Gruppe ein Teiler von 156. Ist andererseits $\ell \in \mathbb{Z}$ mit $\ell \cdot (\bar{1}, \bar{1}, \bar{1}, \bar{1}, \bar{1}) = (\bar{0}, \bar{0}, \bar{0}, \bar{0}, \bar{0})$, dann gilt insbesondere $\ell \cdot (1 + 3\mathbb{Z}) = 0 + 3\mathbb{Z}$, $\ell \cdot (1 + 4\mathbb{Z}) = 0 + 4\mathbb{Z}$ und $\ell \cdot (1 + 13\mathbb{Z}) = 0 + 4\mathbb{Z}$, dann ist $\ell$ ein gemeinsames Vielfaches von 3, 4 und 13, und somit auch von $\mathrm{kgV}(3, 4, 13) = 3 \cdot 4 \cdot 13 = 156$. Daraus folgt, dass $(\bar{1}, ..., \bar{1})$ in der Gruppe ein Element der Ordnung 156 ist. In der Gruppe existiert also ein Element der Ordnung 156, und jede Elementordnung ist ein Teiler von 156, d.h. es gibt keine Elemente größerer Ordnung. Auf Grund der Isomorphie gilt dasselbe für die Elemente der Gruppe $(\mathbb{Z}/2028\mathbb{Z})^\times$.

zu (c) Die Anzahl der Elemente der Ordnung 2 ist gleich 7, und die Anzahl der Elemente der Ordnung 13 ist gleich 12. (Es genügt, die Elementezahlen in der Gruppe $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$ zu bestimmen. Die Elemente der Ordnung 2 sind genau diejenigen mit Einträgen aus $\{\bar{0}, \bar{1}\}$ in den $\mathbb{Z}/2\mathbb{Z}$-Komponenten, mit Einträgen aus $\{\bar{0}, \bar{2}\}$ in der $\mathbb{Z}/4\mathbb{Z}$- Komponente, und mit Eintrag $\bar{0}$ in allen übrigen Komponenten, wobei aber das Nullelement ausgenommen ist. Die Elemente der Ordnung 13 sind genau diejenigen mit einem Eintrag ungleich null in der $\mathbb{Z}/13\mathbb{Z}$-Komponente und Eintrag null in allen übrigen Komponenten.)

Name: _____

**Aufgabe 8.** (4+4+2 Punkte)

Sei $\alpha \in \mathbb{R}$ eine Zahl, die die Gleichung $\alpha^5 = 4\alpha + 2$ erfüllt.

(a) Bestimmen Sie den Erweiterungsgrad $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ (mit Nachweis).

(b) Bestimmen Sie die beiden Erweiterungsgrade $[\mathbb{Q}(\alpha, \sqrt{-3}) : \mathbb{Q}]$ und $[\mathbb{Q}(\alpha, \sqrt{-3}) : \mathbb{Q}(\sqrt{-3})]$ (ebenfalls mit Nachweis).

(c) Begründen Sie, dass kein $\mathbb{Q}$-Homomorphismus $\phi : \mathbb{Q}(\alpha, \sqrt{-3}) \to \mathbb{R}$ existiert.

*Lösung:*

zu (a) Die Gleichung $\alpha^5 - 4\alpha - 2 = 0$ zeigt, dass $\alpha$ eine Nullstelle des Polynoms $f = x^5 - 4x - 2 \in \mathbb{Q}[x]$ ist. Außerdem ist dieses Polynom normiert und irreduzibel auf Grund des Eisenstein-Kriteriums (angewendet auf die Primzahl $p = 2$). Insgesamt gilt damit $\mu_{\alpha,\mathbb{Q}} = f$ und somit $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \mathrm{grad}(f) = 5$.

zu (b) Das Polynom $g = x^2 + 3 \in \mathbb{Q}(\alpha)[x]$ ist normiert und hat $\sqrt{-3}$ als Nullstelle. Wäre es über $\mathbb{Q}(\alpha)$ reduzibel, dann wären die beiden komplexen Nullstellen $\pm\sqrt{-3}$ in $\mathbb{Q}(\alpha)$ enthalten. Aber dies ist nicht der Fall, denn wegen $\alpha \in \mathbb{R}$ gilt $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, während $\pm\sqrt{-3}$ nicht in $\mathbb{R}$ liegen. Insgesamt gilt damit $\mu_{\sqrt{-3},\mathbb{Q}(\alpha)} = g$ und somit

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

Mit der Gradformel erhalten wir

$$[\mathbb{Q}(\alpha, \sqrt{-3}) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\alpha, \sqrt{-3}) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] \quad = \quad 2 \cdot 5 \quad = \quad 10.$$

(Für dieses Ergebnis hätte man auch mit der Teilerfremdheit von 2 und 5 argumentieren können, siehe Übungen.) Als irreduzibles Polynom über $\mathbb{Q}(\alpha)$ ist $g$ wegen $g \in \mathbb{Q}[x]$ auch irreduzibel über $\mathbb{Q}$. Es folgt $g = \mu_{\sqrt{-3},\mathbb{Q}}$ und $[\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}] = \mathrm{grad}(g) = 2$. Eine erneute Anwendung der Gradformel liefert

$$10 \quad = \quad [\mathbb{Q}(\alpha, \sqrt{-3}) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\alpha, \sqrt{-3}) : \mathbb{Q}(\sqrt{-3})] \cdot [\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\alpha, \sqrt{-3}) : \mathbb{Q}(\sqrt{-3})] \cdot 2$$

und schließlich $[\mathbb{Q}(\alpha, \sqrt{-3}) : \mathbb{Q}(\sqrt{-3})] = \frac{10}{2} = 5$.

zu (c) Nehmen wir an, dass ein $\mathbb{Q}$-Homomorphismus $\phi : \mathbb{Q}(\alpha, \sqrt{-3}) \to \mathbb{R}$ existiert. Dann ist $\phi(\sqrt{-3})$ wegen $\phi(\sqrt{-3})^2 = \phi((\sqrt{-3})^2) = \phi(-3) = -3$ eine Nullstelle von $g = x^2 + 3$ in $\mathbb{R}$. Aber wir haben bereits in Teil (b) festgestellt, dass $g$ in $\mathbb{R}$ keine Nullstelle besitzt.