LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Dr. Ralf Gerkmann

Wintersemester 2024/25
14.04.2025

Algebra

(Wiederholungsklausur alte Studienordnung)

Nachschreibklausur

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. (3+4+3 Punkte)

Sei G eine zyklische Gruppe der Ordnung 12 und $g \in G$ ein Element mit $G = \langle g \rangle$. Sei $N = \langle g^4 \rangle$.

(a) Begründen Sie, dass $N \trianglelefteq G$ gilt, und bestimmen Sie die Ordnungen von N und G/N.

(b) Zeigen Sie, dass $R = \{e, g, g^2, g^3\}$ ein Repräsentantensystem von G/N ist.

(c) Begründen Sie, dass $G \cong \mathbb{Z}/12\mathbb{Z}$, $N \cong \mathbb{Z}/3\mathbb{Z}$ und $G/N \cong \mathbb{Z}/4\mathbb{Z}$ gilt.

Lösung:

zu (a) Als zyklische Gruppe ist G abelsch, und daraus folgt, dass jede Untergruppe von G Normalteiler ist. Wegen $4 \mid 12$ gilt $|N| = \mathrm{ord}(g^4) = \frac{12}{4} = 3$, und $|G/N| = \frac{|G|}{|N|} = \frac{12}{3} = 4$.

zu (b) Die Elemente von G/N sind gegeben durch $g^k N$ mit $0 \leq k < 12$. Für jedes solche k liefert die Dimension mit Rest ein $a \in \{0,1,2,3\}$ und ein $q \in \mathbb{Z}$ mit $k = 4q + a$. Wegen $g^{4q} \in N$ gilt $g^k N = g^{a+4q} N = (g^a N)(g^{4q} N) = g^a N$. Dies zeigt, dass das Element $g^a \in R$ in der Nebenklasse $g^k N$ liegt. Andererseits enthält $g^k N$ nicht mehr als ein Elemnt aus R. Sind nämlich $a, b \in \{0,1,2,3\}$ mit $g^a, g^b \in g^k N$, dann folgt $g^a N = g^k N = g^b N$, und daraus wiederum folgt $g^{b-a} \in N$. Wegen $N = \langle g^4 \rangle$ existiert ein $r \in \mathbb{Z}$ mit $g^{b-a} = (g^4)^r = g^{4r}$. Aber wegen $\mathrm{ord}(g) = 12$ ist dann $b - a - 4r$ ein Vielfaches von 12, und 4 somit ein Teiler von $b - a$. Wegen $0 \leq a, b < 4$ folgt daraus wiederum $a = b$.

zu (c) Jede zyklische Gruppe der Ordnung n ist isomorph zu $\mathbb{Z}/n\mathbb{Z}$. Daraus folgt $G \cong \mathbb{Z}/12\mathbb{Z}$. Als zyklische Gruppe der Ordnung 3 ist N isomorph zu $\mathbb{Z}/3\mathbb{Z}$. Die Elemente von G/N sind genau die Elemente der Form $g^k N = (gN)^k$, mit $k \in \mathbb{Z}$. Dies zeigt, dass $G/N = \langle gN \rangle$ gilt, also auch G/N zyklisch ist. Als zyklische Gruppe der Ordnung 4 ist G/N isomorph zu $\mathbb{Z}/4\mathbb{Z}$.

Name: ____________________

Aufgabe 2. (2+3+5 Punkte)

Sei $G = (\mathbb{Z}/16\mathbb{Z}, +)$, und sei $\phi : G \to \mathbb{Z}/4\mathbb{Z}$ die Abbildung definiert durch $\phi(a+16\mathbb{Z}) = a+4\mathbb{Z}$ für alle $a \in \mathbb{Z}$.

(a) Zeigen Sie, dass ϕ ein Gruppenhomomorphismus ist.

(b) Weisen Sie nach, dass ϕ surjektiv ist.

(c) Zeigen Sie, dass ein Isomorphismus $G/\langle 4 + 16\mathbb{Z}\rangle \cong \mathbb{Z}/4\mathbb{Z}$ von Gruppen existiert.

Lösung:

zu (a) Für alle $a, b \in \mathbb{Z}$ gilt

$$\phi((a+16\mathbb{Z})+(b+16\mathbb{Z})) = \phi(a+b+16\mathbb{Z}) = a+b+4\mathbb{Z} = (a+4\mathbb{Z})+(b+4\mathbb{Z}) = \phi(a+16\mathbb{Z})+\phi(b+16\mathbb{Z}).$$

zu (b) Sei $a + 4\mathbb{Z} \in \mathbb{Z}/4\mathbb{Z}$ vorgegeben, mit $a \in \mathbb{Z}$. Dann gilt $\phi(a + 16\mathbb{Z}) = a + 4\mathbb{Z}$.

zu (c) Um den Homomorphiesatz anwenden zu können, müssen wir noch überprüfen, dass $\ker(\phi) = \langle 4 + 16\mathbb{Z}\rangle$ gilt. Die Inklusion „$\supseteq$" ist erfüllt, weil $4 + 16\mathbb{Z}$ wegen $\phi(4+16\mathbb{Z}) = 4+4\mathbb{Z} = 0+4\mathbb{Z} = 0_{\mathbb{Z}/4\mathbb{Z}}$ in $\ker(\phi)$ enthalten ist. Sei umgekehrt $a+16\mathbb{Z}$ ein Element von $\ker(\phi)$, mit $a \in \mathbb{Z}$. Dann gilt $a+4\mathbb{Z} = \phi(a+16\mathbb{Z}) = 0+4\mathbb{Z}$. Es folgt $a \equiv 0 \bmod 4$, es gilt also $a = 4b$ für ein $b \in \mathbb{Z}$. Daraus wiederum folgt $a+16\mathbb{Z} = 4b+16\mathbb{Z} = b(4+16\mathbb{Z}) \in \langle 4+16\mathbb{Z}\rangle$. Der Homomorphiesatz liefert nun den angegebenen Isomorphismus.

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 24 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 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ nicht zu $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ isomorph ist.

(c) Geben Sie zwei nicht abelsche, nicht zueinander isomorphe Gruppen der Ordnung 24 an (mit Nachweis).

Lösung:

zu (a) Die Aussage ist erfüllt für $r = 3$ und $G_1 = \mathbb{Z}/24\mathbb{Z}$, $G_2 = \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ und $G_3 = \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$.

zu (b) Das Element $(\bar{0}, \bar{1})$ ist von Ordnung 8 in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, wegen $12 \cdot (\bar{0}, \bar{1}) = (\bar{0}, \bar{0})$ und $k \cdot (\bar{0}, \bar{1}) \neq (\bar{0}, \bar{0})$ für $1 \leq k \leq 11$. Wären die Gruppen isomorph, dann müsste es auch in $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/1\mathbb{Z}2$ ein Element der Ordnung 8 geben. Es gilt aber $12 \cdot (a, b) = (\bar{0}, \bar{0})$ für alle $(a, b) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, die Ordnung jedes Elements in dieser Gruppe ist also (im Gegensatz zu 8) ein Teiler von 12.

zu (c) Die Gruppen D_{12} und S_4 sind laut Vorlesung beide nicht-abelsch von Ordnung 24. In D_n gibt es für jedes $n \geq 3$ ein Element der Ordnung n, in D_{12} also ein Element der Ordnung 12. In S_4 dagegen existieren neben dem Neutralelement nur Elemente der Ordnung 2, 3 und 4, denn jeder k-Zykel (mit $k \in \{2, 3, 4\}$) ist ein Element der Ordnung k, und die Doppeltranspositionen sind von Ordnung 2. Also sind die beiden Gruppen nicht isomorph.

Name: ____________________

Aufgabe 4. (4+3+3 Punkte)

Sei $G = \mathbb{R}^\times$ mit der Multiplikation als Verknüpfung und $X = \mathbb{R}^3$.

(a) Zeigen Sie, dass durch $\cdot : G \times X \to X$, $(a, v) \mapsto av$ eine Gruppenoperation von G auf X definiert ist.

(b) Bestimmen Sie die Stabilisatorgruppen $G_{(0,0,0)}$ und $G_{(1,1,0)}$ (jeweils mit Nachweis).

(c) Bestimmen Sie die Bahn $G((1, 1, 0))$, und begründen Sie, dass die Operation nicht transitiv ist.

Lösung:

zu (a) Seien $a, b \in \mathbb{R}^\times$ und $v \in \mathbb{R}^3$. Dann gilt $1 \cdot v = 1v = v$ und $a \cdot (b \cdot v) = a(bv) = (ab)v = (ab) \cdot v$.

zu (b) Für jedes $a \in \mathbb{R}^\times$ gilt $a \cdot (0, 0, 0) = (0, 0, 0)$. Somit gilt $G_{(0,0,0)} = \mathbb{R}^\times$. Für jedes $a \in \mathbb{R}^\times$ folgt aus $a \in G_{(1,1,0)}$ jeweils $(a, a, 0) = a \cdot (1, 1, 0) = (1, 1, 0)$, und damit $a = 1$. Dies zeigt, dass $G_{(1,1,0)} = \{1\}$ ist.

zu (c) Nach Definition ist die Bahn gegeben durch

$$G((1, 1, 0)) \quad = \quad \{a \cdot (1, 1, 0) \mid a \in \mathbb{R}^\times\} \quad = \quad \{(a, a, 0) \mid a \in \mathbb{R}^\times\}.$$

Das Element $w = (0, 0, 1)$ stimmt für kein $a \in \mathbb{R}^\times$ mit $(a, a, 0)$ überein. Dies zeigt, dass $G((1, 1, 0))$ nicht mit R^3 übereinstimmt, und somit ist die Operation nicht transitiv.

Name: ______________________________

Aufgabe 5. (4+3+3 Punkte)

Sei G eine Gruppe der Ordnung 2023. (Es ist $2023 = 7 \cdot 17^2$.)

(a) Zeigen Sie, dass G Normalteiler P und Q der Ordnung 7 bzw. 289 besitzt.

(b) Weisen Sie nach, dass $G \cong P \times Q$ gilt.

(c) Begründen Sie, dass G eine abelsche Gruppe ist.

Lösung:

zu (a) Für jede Primzahl p sei ν_p die Anzahl der p-Sylowgruppen von G. Nach dem Dritten Sylowsatz gilt $\nu_{17} \mid 7$, also $\nu_{17} \in \{1, 7\}$, und außerdem $\nu_{17} \equiv 1 \bmod 17$. Wegen $7 \not\equiv 1 \bmod 17$ folgt $\nu_{17} = 1$. Ebenso gilt $\nu_7 \mid 17^2$, also $\nu_7 \in \{1, 17, 17^2\}$, und $\nu_7 \equiv 1 \bmod 7$. Wegen $17 \equiv 3 \not\equiv 1 \bmod 7$ und $17^2 \equiv 3^2 \equiv 9 \equiv 2 \not\equiv 1 \bmod 7$ folgt $\nu_7 = 1$.

Sei sei P die einzige 7 und Q die einzige 17-Sylowgruppe. Wegen $|G| = 7^1 \cdot 17^2$ gilt $|P| = 7$ und $|Q| = 17^2 = 289$. Laut Zweitem Sylowsatz sind P und Q wegen $\nu_7 = \nu_{17} = 1$ beides Normalteiler von G.

zu (b) Laut Vorlesung genügt es nachzuweisen, dass G ein inneres direktes Produkt von P und Q ist. Aus Teil (a) ist bereits bekannt, dass die Untergruppen beides Normalteiler von G sind. Auf Grund der Teilerfremdheit von $|P| = 7$ und $|Q| = 17^2$ gilt $P \cap Q = \{e\}$. Wegen $P, Q \trianglelefteq G$ ist das Komplexprodukt PQ eine Untergruppe von G, sogar ein Normalteiler. Weil P und Q Untergruppen von PQ sind, ist $|PQ|$ nach dem Satz von Lagrange ein gemeinsames Vielfaches von 7 und 17^2, wegen $\mathrm{kgV}(7, 17^2) = 2023$ also ein Vielfaches von $|G|$. Aber aus $PQ \subseteq G$ und $|PQ| \geq |G|$ wiederum folgt $G = PQ$. Insgesamt sind damit alle Eigenschaften eines inneren direkten Produkts nachgewiesen.

zu (c) Als Gruppe der Primzahlordnung 7 ist P zyklisch, somit auch abelsch, und als Gruppe von Primzahlquadratordnung ist Q ebenfalls abelsch. Daraus folgt, dass $P \times Q$ abelsch ist, und auf Grund der Isomorphie ist auch G abelsch.

Name: ______________________________

Aufgabe 6. (4+4+2 Punkte)

Sei $\alpha, \beta \in \mathbb{C}$ mit $\alpha^5 = 4\alpha + 2$ und $\beta^7 = 49\beta + 21$.

(a) Bestimmen Sie die Erweiterungsgrade $[\mathbb{Q}(\alpha) : \mathbb{Q}]$, $[\mathbb{Q}(\beta) : \mathbb{Q}]$ und $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ (jeweils mit Nachweis).

(b) Bestimmen Sie, ebenfalls mit Nachweis, den Grad der Erweiterung $\mathbb{Q}(\alpha, \beta, \sqrt{-3})|\mathbb{Q}$.

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

Lösung:

zu (a) Das Element α ist eine Nullstelle von $f = x^5 - 4x - 2$, und β ist eine Nullstelle von $g = x^7 - 49x - 21$. Die Polynome liegen in $\mathbb{Q}[x]$, sind normiert, und irreduzibel auf Grund des Eisenstein-Kriteriums (angewendet auf die Primzahlen 2 bzw. 7). Es gilt also $\mu_{\alpha,\mathbb{Q}} = f$, $\mu_{\beta,\mathbb{Q}} = g$ und somit $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \mathrm{grad}(f) = 5$, $[\mathbb{Q}(\beta) : \mathbb{Q}] = \mathrm{grad}(g) = 7$.

Der Körper $\mathbb{Q}(\alpha)$ und $\mathbb{Q}(\beta)$ sind Zwischenkörper von $\mathbb{Q}(\alpha, \beta) \mid \mathbb{Q}$. Auf Grund der Gradformel gilt

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \cdot 5$$

und

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)] \cdot 7.$$

Dies zeigt, dass $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ ein Vielfaches von $\mathrm{kgV}(5, 7) = 35$ ist, und insbesondere $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \geq 35$ gilt. Das Polynom g liegt auch in $\mathbb{Q}(\alpha)[x]$, ist wegen $g(\beta) = 0$ also ein Vielfaches von $\mu_{\beta,\mathbb{Q}(\alpha)}$. Daraus folgt $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)] = \mathrm{grad}(\mu_{\beta,\mathbb{Q}(\alpha)}) \leq \mathrm{grad}(g) = 7$. Eine nochmalige Anwendung der Gradformel liefert

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 7 \cdot 5 \quad = \quad 35$$

und insgesamt $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 35$.

zu (b) Das Polynom $h = x^2 + 1$ liegt in $\mathbb{Q}(\alpha, \beta)[x]$, ist normiert und hat $\sqrt{-3}$ als Nullstelle. Wäre es reduzibel, dann würden $\pm\sqrt{-3}$ wegen $\mathrm{grad}(h) = 2$ in $\mathbb{Q}(\alpha, \beta)$ liegen. Es wäre dann $\mathbb{Q}(\sqrt{-3})$ ein Zwischenkörper von $\mathbb{Q}(\alpha, \beta) \mid \mathbb{Q}$. Laut Vorlesung gilt $[\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}] = 2$. Auf Grund der Gradformel

$$35 \quad = \quad [\mathbb{Q}(\alpha, \beta, \sqrt{-3}) : \mathbb{Q}(\sqrt{-3})] \cdot [\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\alpha, \beta, \sqrt{-3}) : \mathbb{Q}(\sqrt{-3})] \cdot 2$$

wäre 2 ein Teiler von 35. Der Widerspruch zeigt, dass h über $\mathbb{Q}(\alpha, \beta)$ irreduzibel ist. Insgesamt gilt $h = \mu_{\sqrt{-3},\mathbb{Q}(\alpha,\beta)}$ und $[\mathbb{Q}(\alpha, \beta, \sqrt{-3}) : \mathbb{Q}(\alpha, \beta)] = \mathrm{grad}(h) = 2$. Mit der Gradformel erhalten wir

$$[\mathbb{Q}(\alpha, \beta, \sqrt{-3}) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\alpha, \beta, \sqrt{-3}) : \mathbb{Q}(\alpha, \beta)] \cdot [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \quad = \quad 2 \cdot 35 \quad = \quad 70.$$

zu (c) Angenommen, $\phi : \mathbb{Q}(\alpha, \beta) \to \mathbb{Q}$ ist ein $\mathbb{Q}$-Homomorphismus. Dann bildet ϕ die Nullstelle α von f auf eine Nullstelle $\phi(\alpha)$ von f in $\mathbb{Q}$ ab. Aber aus Teil (a) ist bekannt, dass f in $\mathbb{Q}[x]$ irreduzibel ist und somit keine rationale Nullstelle besitzt. Der Widerspruch zeigt, dass kein $\mathbb{Q}$-Homomorphismus wie angegeben existiert.

Name: ______________________________

Aufgabe 7. (2+4+4 Punkte)

Es sei $\mathbb{F}_2^{\mathrm{alg}}$ ein algebraischer Abschluss des Körpers $\mathbb{F}_2$. Für jedes $n \in \mathbb{N}$ sei $\mathbb{F}_{2^n}$ der eindeutig bestimmte Zwischenkörper von $\mathbb{F}_2^{\mathrm{alg}}|\mathbb{F}_2$ mit 2^n Elementen.

(a) Bestimmen Sie die Anzahl der Teilkörper von $\mathbb{F}_{64}$.

(b) Bestimmen Sie die Anzahl der Elemente $\alpha \in \mathbb{F}_{16}^\times$ mit $\langle \alpha \rangle = \mathbb{F}_{16}^\times$.

(c) Bestimmen Sie die Anzahl der Elemente in $\mathbb{F}_4 \cup \mathbb{F}_8$.

Lösung:

zu (a) Es gilt $[\mathbb{F}_{64} : \mathbb{F}_2] = [\mathbb{F}_{2^6} : \mathbb{F}_2] = 6$. Die Zahl 6 besitzt vier Teiler (1, 2, 3 und 6). Laut Vorlesung stimmt diese Anzahl mit der Anzahl der Teilkörper von $\mathbb{F}_{64}$ überein.

zu (b) Die Gruppe $\mathbb{F}_{16}^\times$ ist von Ordnung 15, und als multiplikative Gruppe eines endlichen Körpers auch zyklisch. Eine zyklische Gruppe der Ordnung 15 besitzt laut Vorlesung genau $\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$ erzeugende Elemente.

zu (c) Für alle $m, n \in \mathbb{N}$ ist $m \mid n$ äquivalent zu $\mathbb{F}_{2^m} \subseteq \mathbb{F}_{2^n}$. Die Zahl 1 ist der einzige gemeinsame Teiler von 2 und 3, und somit ist $\mathbb{F}_2$ der einzige gemeinsame Teilkörper von $\mathbb{F}_4 = \mathbb{F}_{2^2}$ und $\mathbb{F}_8 = \mathbb{F}_{2^3}$. Da $\mathbb{F}_4 \cap \mathbb{F}_8$ ein gemeinsamer Teilkörper der beiden Körper ist, folgt $\mathbb{F}_4 \cap \mathbb{F}_8 = \mathbb{F}_2$. Daraus wiederum folgt

$$|\mathbb{F}_4 \cup \mathbb{F}_8| \quad = \quad |\mathbb{F}_4| + |\mathbb{F}_8| - |\mathbb{F}_4 \cap \mathbb{F}_8| \quad = \quad 4 + 8 - 2 \quad = \quad 10.$$

Name: ______________________________

Aufgabe 8. (4+3+3 Punkte)

Sei $\alpha = \sqrt{4+5\sqrt{2}}$.

(a) Bestimmen Sie das Minimalpolynom des Elements α über $\mathbb{Q}$ (mit Nachweis).

(b) Bestimmen Sie das Minimalpolynom von α über $\mathbb{Q}(\sqrt{2})$.
Hier ist *kein* Nachweis erforderlich.

(c) Begründen Sie, dass $\mathbb{Q}(\alpha)|\mathbb{Q}$ keine normale Erweiterung ist.

Lösung:

zu (a) Es gilt

$$\alpha = \sqrt{4+5\sqrt{2}} \quad\Rightarrow\quad \alpha^2 = 4+5\sqrt{2} \quad\Rightarrow\quad \alpha^2 - 4 = 5\sqrt{2} \quad\Rightarrow\quad (\alpha^2-4)^2 = 50$$
$$\Rightarrow\quad \alpha^4 - 8\alpha^2 + 16 = 50 \quad\Rightarrow\quad \alpha^4 - 8\alpha^2 - 34 = 0.$$

Das Element α ist also eine Nullstelle von $f = x^4 - 8x^2 - 34$. Außerdem ist das Polynom normiert, und irreduzibel auf Grund des Eisenstein-Kriteriums (angewendet auf die Primzahl 2). Ingesamt folgt daraus $\mu_{\alpha,\mathbb{Q}} = f$.

zu (b) Es gilt $\mu_{\alpha,\mathbb{Q}(\sqrt{2})} = x^2 - (4+5\sqrt{2})$.

zu (c) Das Polynom f ist in $\mathbb{Q}[x]$ irreduzibel und besitzt mit α in $\mathbb{Q}(\alpha)$ eine Nullstelle. Wäre $\mathbb{Q}(\alpha)|\mathbb{Q}$ normal, dann müsste f über $\mathbb{Q}(\alpha)$ in Linearfaktoren zerfallen. Alle komplexen Nullstellen von f müssten somit in $\mathbb{Q}(\alpha)$ liegen. Nun ist auch $\beta = \sqrt{4-5\sqrt{2}}$ eine Nullstelle von f, denn es gilt

$$f(\beta^4) \quad=\quad (4-5\sqrt{2})^2 - 8\cdot(4-5\sqrt{2}) - 34 \quad=\quad 16 - 40\sqrt{2} + 50 - 32 + 40\sqrt{2} - 34 \quad=\quad 0.$$

Aber wegen $4 - 5\sqrt{2} < 0$ ist β nicht reell, kann somit wegen $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ auch nicht in $\mathbb{Q}(\alpha)$ liegen.