

Algebra
Hauptklausur
Lösungsvorschlag

Aufgabe 1.

- a) Die Ordnung eines Elements muss 12 teilen, also kann es nur 1, 2, 3, 4, 6, oder 12 sein.
- b) In $\mathbb{Z}/12\mathbb{Z}$ gilt $\text{ord}(\overline{1}) = 12$, $\text{ord}(\overline{2}) = 6$, $\text{ord}(\overline{3}) = 4$, $\text{ord}(\overline{4}) = 3$, $\text{ord}(\overline{6}) = 2$, und $\text{ord}(\overline{12}) = 1$.
- c) Sei $a = (g, g') \in G \times G'$. Dann gilt $a^6 = (g^6, g'^6)$. Da $\#G = 2$, gilt $g^2 = e_G$, also $g^6 = (g^2)^3 = e_G^3 = e_G$. Da $\#G' = 6$, gilt $g'^6 = e_{G'}$. Daraus folgt, dass $a^6 = (e_G, e_{G'}) = e_{G \times G'}$.
- d) Seien $\sigma = \overline{12} \in S_2$ und $\tau = \overline{123} \in S_3$, und sei $a = (\sigma, \tau) \in S_2 \times S_3$. Dann ist $a \neq (\text{id}, \text{id})$, $a^2 = (\text{id}, \overline{321}) \neq (\text{id}, \text{id})$, $a^3 = (\overline{12}, \text{id}) \neq (\text{id}, \text{id})$, und $a^6 = (\text{id}, \text{id})$.
- e) In A_4 liegen:
- id , welches Ordnung 1 hat,
 - 3 Elemente der Form $\overline{ab\,cd}$, die Ordnung 2 haben,
 - und 8 Elemente der Form $\overline{123} = \overline{12\,23}$, die Ordnung 3 haben.

Es gilt $\#A_4 = 12$, also sind das alle Elemente in A_4 und es gibt keine weitere Ordnung.

Aufgabe 2.

- a) Aus den Sylow-Sätzen folgt, dass $\#P_{11} = 11^2$.
- b) Sei s_{11} der Anzahl der Sylow-11-Untegruppe von G . Aus den Sylow-Sätzen folgt, dass $s_{11} \equiv 1 \pmod{11}$ ist und $s_{11} | 15$ gilt, also $s_{11} \in \{1, 3, 5, 15\}$, von wem die einzige Zahl gleich 1 mod 11 ist 1, also $s_{11} = 1$ und P_{11} ist ein Normalteiler von G .
- c) Es gilt $\#(G/P_{11}) = \frac{\#G}{\#P_{11}} = \frac{3 \cdot 5 \cdot 11^2}{11^2} = 3 \cdot 5$. Also $\#Q_5 = 5$. Sei s_5 der Anzahl der Sylow-5-Untegruppen von G/P_{11} . Dann ist $s_5 \equiv 1 \pmod{5}$ und gilt $s_5 | 3$, also $s_5 \in \{1, 3\}$, von wem die einzige Zahl gleich 1 mod 5 ist 1, also $s_5 = 1$ und Q_5 ist ein Normalteiler von G/P_{11} .
- d) Wir betrachten $\pi|_N : N \rightarrow G/P_{11}$. Es gilt $\text{im}(\pi|_N) = \pi(N) = Q_5$ und $\ker(\pi|_N) = P_{11}$, daraus folgt $N/\ker(\pi|_N) \cong \text{im}(\pi|_N)$, also $N/P_{11} \cong Q_5$. Aus Lagrange folgt $\#N = \#P_{11}\#Q_5 = 11^2 \cdot 5$, da $\#Q_5 = 5$ weil Q_5 eine Sylow-5-Untergruppe ist.
- e) Wir müssen zeigen, dass P_{11} ein Normalteiler von N ist, dass N ein Normalteiler von G ist, und dass G/N , N/P_{11} und P_{11} abelsch sind.

- P_{11} ist ein Normalteiler von G (aus b)). Es gilt $P_{11} = \ker(\pi) = \pi^{-1}(e_{G/P_{11}}) \subseteq \pi^{-1}(Q_5) = N$, also $P_{11} \subseteq N$ und P_{11} ist ein Normalteiler von N .
- Q_5 ist ein Normalteiler von G/P_{11} , also ist $N = \pi^{-1}(Q_5)$ ein Normalteiler von $\pi^{-1}(G/P_{11}) = G$.
- Es gilt $\#P_{11} = 11^2$, und alle Gruppen der Ordnung 11^2 sind abelsch.
- Es gilt $N/P_{11} = \pi(N) = Q_5$, also $\#(N/P_{11}) = \#Q_5 = 5$, und alle Gruppen der Ordnung 5 sind abelsch.
- Schließlich gilt $\#(G/N) = \frac{\#G}{\#N} = \frac{3 \cdot 5 \cdot 11^2}{5 \cdot 11^2} = 3$, und alle Gruppen der Ordnung 3 sind abelsch.

Aufgabe 3.

- Die Primfaktorzerlegung von f ist $x^3(x^2 + 1)$, denn in $\mathbb{R}[x]$ ist x irreduzibel, weil es Grad 1 hat, und $x^2 + 1$ ist irreduzibel, weil es keine Nullstelle in $\mathbb{R}$ hat.
- Es gilt $f \in (x)$, und $f \in (x^2 + 1)$. Die sind maximal, weil die erzeugt von irreduzibel Elemente sind.
- Sei $\mathfrak{a}$ ein Maximales Ideal, das f enthält. Da $\mathbb{R}[x]$ ein Hauptidealring ist, gilt $\mathfrak{a} = (h)$ mit h irreduzibel. Also gilt $h|f$ und h ist irreduzibel, dass heißt, entweder $h = x$ oder $h = x^2 + 1$ (wegen Eindeutigkeit der Primfaktorzerlegung).
- Da $\mathbb{R}[x]$ ein Hauptidealring ist, existiert $h \in \mathbb{R}[x]$ mit $(f, g) = (h)$, also $h|f$ und $h|g$. Aber die Primfaktorzerlegung von g ist $g = x(x^2 - 2) = x(x - \sqrt{2})(x + \sqrt{2})$, also $\text{ggT}(f, g) = x$ und $(f, g) = (x)$.

Alternativ Lösung: Es gilt $f = (x^2 + 3)g - 6x$, also $x = \frac{(x^2+3)}{6}g - \frac{1}{6}f \in (f, g)$ und $(x) \subseteq (f, g)$. Aber $x|f$ und $x|g$, also $(f, g) \subseteq (x)$, das heißt, $(f, g) = (x)$.

- Sei $h = \text{kgV}(f, g) = x^3(x^2 + 1)(x - \sqrt{2})(x + \sqrt{2})$, also $(f) \cap (g) = (h)$.

Aufgabe 4.

- Wir benutzen das Eisensteins Kriterium mit $p = 3$: es gilt $3 \nmid 1$, $3|9$, $3|12$ und $3^2 \nmid 12$; also ist $x^5 - 9x - 12$ irreduzibel über $\mathbb{Q}$.
- Da $f(a) = 0$ und f irreduzibel über $\mathbb{Q}$ ist, gilt $[\mathbb{Q}(a) : \mathbb{Q}] = 5$.
- Es gilt $ra + a^2 \in \mathbb{Q}(a)$, also $\mathbb{Q} \subseteq \mathbb{Q}(ra + a^2) \subseteq \mathbb{Q}(a)$ und $5 = [\mathbb{Q}(a) : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}(ra + a^2)][\mathbb{Q}(ra + a^2) : \mathbb{Q}]$. Es gilt $ra + a^2 \notin \mathbb{Q}$; sonst ist $x^2 + rx - (a^2 + ra) \in \mathbb{Q}[x]$ ein Polynom, das a annulliert, und es gilt $[\mathbb{Q}(a) : \mathbb{Q}] \leq 2$. Also gilt $[\mathbb{Q}(ra + a^2) : \mathbb{Q}] > 1$, und da der Grad 5 teilt, gilt $[\mathbb{Q}(ra + a^2) : \mathbb{Q}] = 5$.

Alternativ Lösung: Da $[\mathbb{Q}(a) : \mathbb{Q}] = 5$, gilt $\mathbb{Q}(a) = \{r_0 + r_1a + r_2a^2 + r_3a^3 + r_4a^4 \mid r_0, \dots, r_4 \in \mathbb{Q}\}$. Insbesondere, $ra + a^2 \in \mathbb{Q}(a)$, und $ra + a^2 \notin \mathbb{Q}$. Daraus folgt $[\mathbb{Q}(ra + a^2) : \mathbb{Q}] > 1$ und $5 = [\mathbb{Q}(a) : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}(ra + a^2)][\mathbb{Q}(ra + a^2) : \mathbb{Q}]$, also $[\mathbb{Q}(ra + a^2) : \mathbb{Q}] = 5$.

- Da $\sqrt[3]{r'} \in \mathbb{Q}(a)$, gilt $\mathbb{Q}(\sqrt[3]{r'}) \subseteq \mathbb{Q}(a)$, also $5 = [\mathbb{Q}(a) : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}(\sqrt[3]{r'})][\mathbb{Q}(\sqrt[3]{r'}) : \mathbb{Q}]$. Das Polynom $x^3 - r'$ annulliert $\sqrt[3]{r'}$, also $[\mathbb{Q}(\sqrt[3]{r'}) : \mathbb{Q}] \leq 3$. Aber $[\mathbb{Q}(\sqrt[3]{r'}) : \mathbb{Q}]$ teilt 5, also, $[\mathbb{Q}(\sqrt[3]{r'}) : \mathbb{Q}] = 1$ und $\sqrt[3]{r'} \in \mathbb{Q}$.

- e) Da f irreduzibel ist, sind alle seine Nullstelle paarweise verschiedene, also hat f in $\mathbb{C}$ mehrere Nullstelle $\neq b$; sei c eine solche Nullstelle, es gilt $c \in \mathbb{C} \setminus \mathbb{R}$. Also $c \notin \mathbb{R} \supseteq \mathbb{Q}(b)$, das heißt, $\mathbb{Q}(b)$ enthält nicht alle Nullstellen von f , und ist nicht der Zerfällungskörper von f .
- f) Sei L der Zerfällungskörper von f . Aus e) folgt, dass $[L : \mathbb{Q}(b)] > 1$ ist, also $[L : \mathbb{Q}] = [L : \mathbb{Q}(b)][\mathbb{Q}(b) : \mathbb{Q}] > 5$. Da b' eine Nullstelle von f ist, gilt $[\mathbb{Q}(c) : \mathbb{Q}] = 5$, also $\mathbb{Q}(c) \neq L$.

Aufgabe 5.

- a) Ja, da $\text{MiPo}_{\zeta_7/\mathbb{Q}} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, und die Nullstellen davon sind $\zeta_7, \zeta_7^2, \zeta_7^3, \zeta_7^4, \zeta_7^5$ und ζ_7^6 , die alle in $\mathbb{Q}(\zeta_7)$ liegen.
- b) Es gilt $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6$, also eine Basis von $\mathbb{Q}(\zeta_7)$ als $\mathbb{Q}$ -Vektorraum ist $\{1, \zeta_7, \zeta_7^2, \zeta_7^3, \zeta_7^4, \zeta_7^5\}$.
- c) Es gilt $1 + \zeta_7 + \zeta_7^2 + \zeta_7^3 + \zeta_7^4 + \zeta_7^5 + \zeta_7^6 = 0$, also $\zeta_7^6 = -\zeta_7^5 - \zeta_7^4 - \zeta_7^3 - \zeta_7^2 - \zeta_7 - 1$ und $a = \zeta_7 + \zeta_7^6 = -\zeta_7^5 - \zeta_7^4 - \zeta_7^3 - \zeta_7^2 - 1$.
- d) Es gilt $\zeta_7^6 \zeta_7 = \zeta_7^7 = 1$, also $\zeta_7^6 = \zeta_7^{-1}$. Daraus folgt $\sigma(\zeta_7) = \zeta_7^6 = \zeta_7^{-1}$, $a = \zeta_7 + \zeta_7^{-1}$, und $\sigma(a) = \sigma(\zeta_7) + \sigma(\zeta_7)^{-1} = \zeta_7^{-1} + (\zeta_7^{-1})^{-1} = \zeta_7^{-1} + \zeta_7 = a$.
- e) Es gilt $\sigma^2(\zeta_7) = \sigma(\zeta_7^{-1}) = \zeta_7$, also ist σ^2 die Identität auf $\mathbb{Q}(\zeta_7)$. Es gilt $\#\langle \sigma \rangle = 2$. Aus der Hauptsatz der Galois-Theorie folgt $[\mathbb{Q}(\zeta_7) : F] = 2$, und $6 = [\mathbb{Q}(\zeta_7) : \mathbb{Q}] = [\mathbb{Q}(\zeta_7) : F][F : \mathbb{Q}] = 2[F : \mathbb{Q}]$, also $[F : \mathbb{Q}] = 3$.
- f) Es gilt $\sigma(a) = a$, also $a \in F$ und $\mathbb{Q}(a) \subseteq F$. Daraus folgt, dass $3 = [F : \mathbb{Q}] = [F : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}] = [F : \mathbb{Q}(a)] \cdot 3$, also $[F : \mathbb{Q}(a)] = 1$ und $F = \mathbb{Q}(a)$.