

Algebra
Probeklausur
Lösungsvorschlag

Aufgabe 1.

- a) Sei $n \in \mathbb{Z}$. Es gilt $f(n) = (-1)^n$. Daraus folgt, dass $f(n+m) = (-1)^{n+m} = (-1)^n \cdot (-1)^m = f(n)f(m)$ gilt für jede $n, m \in \mathbb{Z}$.
- b) Es gilt $f(n) = 1$ genau dann, wenn n gerade ist, also $\ker(f) = 2\mathbb{Z}$.
- c) Angenommen, dass $g: \mathbb{Q} \rightarrow \mathbb{R}^\times$ existiert, mit $g(n) = f(n)$ für alle $n \in \mathbb{Z}$. Insbesondere, $g(1) = -1$. Dann ist $-1 = g(1) = g(\frac{1}{2} + \frac{1}{2}) = g(\frac{1}{2})g(\frac{1}{2}) = g(\frac{1}{2})^2$, also $g(\frac{1}{2})^2 = -1$ und $g(\frac{1}{2}) \notin \mathbb{R}$.
- d) Seien $n, m \in \mathbb{Z}$. Dann gilt $1 = g(2n) = g(n)^2 = g(m \frac{n}{m})^2 = g(\frac{n}{m})^{2m}$, also $g(\frac{n}{m})^{2m} = 1$ und $g(\frac{n}{m})$ ist ein Einheitswurzel.

Aufgabe 2.

- a) Es gilt $\text{ord}(\widehat{12\,4567}) = \text{kgV}(2, 4) = 4$.

Alternativ Lösung: Es gilt $(\widehat{12\,4567})^2 = \widehat{46\,57} \neq \text{id}$, $(\widehat{12\,4567})^3 = \widehat{12\,4765} \neq \text{id}$, und $(\widehat{12\,4567})^4 = \text{id}$, also ist die Ordnung 4.

- b) Nein: Sei $\sigma \in S_7$ und seien $\sigma_1, \dots, \sigma_k$ die Zyklen in der Zykelzerlegung von σ , und sei n_i der Länge der Zyklus σ_i . Dann gilt $\text{ord}(\sigma) = \text{kgV}(n_1, \dots, n_k)$ und jede $n_i \leq 7$ ist. Insbesondere, $\text{ord}(\sigma) \mid \text{kgV}(1, 2, \dots, 7) = 2^2 \cdot 3 \cdot 5 \cdot 7 = 420$, und $8 \nmid 420$.

- c) Da $\widehat{123}$ und $\widehat{456}$ disjunkt Trägern haben, die kommutieren, und ist daraus H abelsch. Es gilt auch $\text{ord}(\widehat{123}) = \text{ord}(\widehat{456}) = 3$. Daraus folgt $H = \left\{ \widehat{123}^i \widehat{456}^j \mid 0 \leq i, j \leq 2 \right\}$ und $\#H = 3^2 = 9$.

Da $\#S_7 = 3^2 \cdot (2^4 \cdot 5 \cdot 7)$, die Sylow-3-Untergruppen von S_7 sind genau die Untergruppen der Ordnung $3^2 = 9$. Also ist H eine Sylow-3-Untergruppe von S_7 .

- d) Seien $\tau_1 = \sigma \widehat{123} \sigma^{-1} = \widehat{34\,67\,123\,76\,43} = \widehat{124}$ und $\tau_2 = \sigma \widehat{456} \sigma^{-1} = \widehat{34\,67\,456\,76\,43} = \widehat{357}$. Es gilt $\sigma H \sigma^{-1} = \sigma \langle \widehat{123}, \widehat{456} \rangle \sigma^{-1} = \langle \sigma \widehat{123} \sigma^{-1}, \sigma \widehat{456} \sigma^{-1} \rangle = \langle \tau_1, \tau_2 \rangle$.

- e) Bei der Sylow-Sätze gilt, dass alle Sylow-3-Untegruppe konjugiert zu einanders sind. Sei P_3 ein Sylow-3-Untegruppe, dann existiert $\tau \in S_7$ mit $P_3 = \tau H \tau^{-1} = \langle \tau \widehat{123} \tau^{-1}, \tau \widehat{456} \tau^{-1} \rangle = \langle \widehat{\tau(1)\tau(2)\tau(3)}, \widehat{\tau(4)\tau(5)\tau(6)} \rangle$.

Aufgabe 3.

- a)
 - Es gilt $0 = 0 + 0i \in R$.
 - Sei $z = a + ib \in R$, dann gilt $-z = -a - ib \in R$.
 - Seien $x = a + ib \in R$ und $y = c + id \in R$. Dann gilt $x + y = (a + c) + (b + d)i \in R$.
 - Seien $x = a + ib \in R$ und $y = c + id \in R$. Dann gilt $xy = ac + adi + bci - bd = (ac - bd) + i(ad + bc) \in R$.
- b) Sei $x = a + ib \in \mathfrak{a}$. Dann existiert $z = c + id \in R$ mit $x = 2z$, also $a = 2c \in 2\mathbb{Z}$ und $b = 2d \in 2\mathbb{Z}$. Sei nun $y = a + ib$ mit $a, b \in 2\mathbb{Z}$. Dann existieren $c, d \in \mathbb{Z}$ mit $a = 2c$ und $b = 2d$. Daraus folgt, dass $y = 2(c + id) \in \mathfrak{a}$, also $\mathfrak{a} = 2\mathbb{Z}[i] = \{2a + 2ib \mid a, b \in \mathbb{Z}\}$.
- c) Sei $x = a + ib \in R$.
- Wenn a, b beide gerade sind, dann ist $x \in \mathfrak{a}$ und $\bar{x} = 0 \in R/\mathfrak{a}$.
 - Wenn $a = 2a'$ gerade ist und $b = 2b' + 1$ ungerade ist, dann ist $x = 2a' + 2b'i + i = 2(a' + b'i) + i$ und $\bar{x} = \bar{i} \in R/\mathfrak{a}$.
 - Wenn a ungerade ist und b gerade ist, gilt ähnlich $\bar{x} = \bar{1} \in R/\mathfrak{a}$.
 - Zuletzt, wenn a, b beide ungerade sind, gilt $\bar{x} = \overline{1 + i}$.

Also $R/\mathfrak{a} = \{\bar{0}, \bar{1}, \bar{i}, \overline{1 + i}\}$. Da $1, i$ und $1 + i$ nicht in $\mathfrak{a}$ liegen, gelten $\bar{0} \neq \bar{1}, \bar{0} \neq \bar{i}$ und $\bar{0} \neq \overline{1 + i}$ in $R/\mathfrak{a}$. Aus $\bar{1} \neq \bar{0}$ folgt $\overline{1 + i} \neq \bar{i}$ und aus $\bar{0}i \neq \bar{0}$ folgt $\overline{1 + i} \neq \bar{1}$. Schließlich gilt $\bar{1} \neq \bar{i}$ da $1 - i \notin \mathfrak{a}$ liegt. Also sind alle Elemente in $\{\bar{0}, \bar{1}, \bar{i}, \overline{1 + i}\}$ paarweiseverschiedene, und es gilt $\#R/\mathfrak{a} = 4$.

- d) Es gilt $\overline{1 + i} \neq \bar{0}$ und $\overline{(1 + i)(1 + i)} = \overline{1 + 2i - 1} = \overline{2i} = \bar{0}$.
- e) Da $R/\mathfrak{a}$ ein Nullteiler besitzt, ist er kein Körper, und daraus folgt, dass $\mathfrak{a}$ nicht maximal ist. Das heißt, es existiert ein Ideal $\mathfrak{b} \triangleleft R$ mit $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq R$.
- f) Es gilt $R/\mathfrak{b} \cong (R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a})$.

(Beweis davon: Da $\mathfrak{a} \subseteq \mathfrak{b}$ gilt, ist $\mathfrak{b}/\mathfrak{a} = \{\bar{x} \mid x \in \mathfrak{b}\} \subseteq R/\mathfrak{a}$ ein Ideal von $R/\mathfrak{a}$. Wir betrachten die kanonische Abbildungen $f: R \rightarrow R/\mathfrak{a}$ und $g: R/\mathfrak{a} \rightarrow (R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a})$, und wir setzen $h = f \circ g$. Es gilt $\ker(h) = f^{-1}(\ker(g))$, $\ker(g) = \mathfrak{b}/\mathfrak{a}$, und $f^{-1}(\mathfrak{b}/\mathfrak{a}) = \mathfrak{b}$, also $\ker(h) = \mathfrak{b}$. Daraus folgt $R/\ker(h) = R/\mathfrak{b} \equiv \text{im}(h) = (R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a})$.)

Daraus folgt $\#(R/\mathfrak{b}) = \frac{\#(R/\mathfrak{a})}{\#(\mathfrak{b}/\mathfrak{a})}$; insbesondere, $\#(R/\mathfrak{b}) \mid 4$. Da $\mathfrak{b} \neq \mathfrak{a}$, gilt $\#(R/\mathfrak{b}) \neq 4$. Da $\mathfrak{b} \neq R$, gilt $\#(R/\mathfrak{b}) \neq 1$. Also muss $\#(R/\mathfrak{b}) = 2$ und $R/\mathfrak{b} \cong \mathbb{F}_2$.

Alternativ Lösung: Da $\mathfrak{a} \subsetneq \mathfrak{b}$ gilt, existiert $x = a + ib \in \mathfrak{b} \setminus \mathfrak{a}$. Wenn b gerade ist, ist a ungerade. Es gilt $ib \in 2i\mathbb{Z} \subseteq \mathfrak{a} \subseteq \mathfrak{b}$ und $x - ib = a \in \mathfrak{b}$. Da a ungerade ist, ist $a = 2a' + 1$ mit $a' \in \mathbb{Z}$, also $2a' \in \mathfrak{a} \subseteq \mathfrak{b}$ und $a - 2a' = 1 \in \mathfrak{b}$. Aber $\mathfrak{b} \neq R$ und $1 \notin \mathfrak{b}$; daraus folgt, dass b ungerade ist, also $b = 2b' + 1$ mit $b' \in \mathbb{Z}$. Da $2b'i \in \mathfrak{a} \subseteq \mathfrak{b}$ ist, gilt $x - 2b'i = a + i \in \mathfrak{b}$.

Sei $y = c + di \in R$. Es gilt $d(a + i) \in \mathfrak{b}$, also $y \equiv y - d(a + i) \equiv c - da \pmod{\mathfrak{b}}$; das heißt, es existiert $c' \in \mathbb{Z}$ mit $\bar{y} = \bar{c}' \in R/\mathfrak{b}$. Daraus folgt, dass $R/\mathfrak{b} = \{\bar{0}, \bar{1}\} \cong \mathbb{F}_2$.

Aufgabe 4.

- a)
 - $\sqrt{5}$ ist eine Nullstelle des Polynoms $x^2 - 5$, das irreduzibel über $\mathbb{Q}$ ist aus Eisensteinskriterium. Also gilt $\text{MiPo}_{\sqrt{5}/\mathbb{Q}} = x^2 - 5$ und $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$.
 - $\sqrt[3]{5}$ ist eine Nullstelle des Polynoms $x^3 - 5$, das irreduzibel über $\mathbb{Q}$ ist aus Eisensteinskriterium. Also gilt $\text{MiPo}_{\sqrt[3]{5}/\mathbb{Q}} = x^3 - 5$ und $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$.

b) Angenommen, dass $\sqrt{5} \in \mathbb{Q}(\sqrt[3]{5})$ liegt. Dann gilt $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\sqrt[3]{5})$, und $3 = [\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}(\sqrt{5})] \cdot 2$, aber $2 \nmid 3$. Daraus folgt, dass $\sqrt{5} \notin \mathbb{Q}(\sqrt[3]{5})$ liegt.

c) Es gilt $\sqrt{5} \notin \mathbb{Q}(\sqrt[3]{5})$, also $[\mathbb{Q}(\sqrt{5}, \sqrt[3]{5}) : \mathbb{Q}(\sqrt[3]{5})] > 1$. $\sqrt{5}$ ist eine Nullstelle des Polynoms $x^2 - 5$, also $\deg(\text{MiPo}_{\sqrt{5}/\mathbb{Q}(\sqrt[3]{5})}) \leq 2$ und $[\mathbb{Q}(\sqrt{5}, \sqrt[3]{5}) : \mathbb{Q}(\sqrt[3]{5})] \leq 2$. Daraus folgt $[\mathbb{Q}(\sqrt{5}, \sqrt[3]{5}) : \mathbb{Q}(\sqrt[3]{5})] = 2$.

Alternativ Lösung: $\sqrt{5}$ ist eine Nullstelle des Polynoms $x^2 - 5$. Die Nullstellen davon sind $\sqrt{5}$ und $-\sqrt{5}$, die beide nicht in $\mathbb{Q}(\sqrt[3]{5})$ liegen. Also ist $x^2 - 5$ ein Polynom der Grad 2 ohne Nullstelle in $\mathbb{Q}(\sqrt[3]{5})$, und daraus ist es irreduzibel über $\mathbb{Q}(\sqrt[3]{5})$. Also gilt $\text{MiPo}_{\sqrt{5}/\mathbb{Q}(\sqrt[3]{5})} = x^2 - 5$ und $[\mathbb{Q}(\sqrt{5}, \sqrt[3]{5}) : \mathbb{Q}(\sqrt[3]{5})] = 2$.

d) Es gilt $[\mathbb{Q}(\sqrt{5}, \sqrt[3]{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{5}, \sqrt[3]{5}) : \mathbb{Q}(\sqrt[3]{5})][\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 2 \cdot 3 = 6$.

e) Es gilt $\sqrt{5} = b^3$ und $\sqrt[3]{5} = b^2$.

Sei $x \in \mathbb{Q}(\sqrt{5}, \sqrt[3]{5})$. Wir setzen $K = \mathbb{Q}(\sqrt[3]{5})$, dann $\mathbb{Q}(\sqrt{5}, \sqrt[3]{5}) = K(\sqrt{5})$. Da $[K(\sqrt{5}) : K] = 2$, existieren $a, a' \in K$ mit $x = a + a'\sqrt{5}$. Da $a \in K = \mathbb{Q}(\sqrt[3]{5})$ und da $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$, existieren $a_0, a_2, a_4 \in \mathbb{Q}$ mit $a = a_0 + a_2\sqrt[3]{5} + a_4\sqrt[3]{5}^2$. Ähnlich, da $a' \in \mathbb{Q}(\sqrt[3]{5})$ liegt, existieren $a_3, a_5, b_1 \in \mathbb{Q}$ mit $a' = a_3 + a_5\sqrt[3]{5} + a_7\sqrt[3]{5}^2$. Wir setzen $a_1 = \frac{b_1}{5}$. Schließlich gilt $x = a + a'\sqrt{5} = a_0 + a_2\sqrt[3]{5} + a_4\sqrt[3]{5}^2 + (a_3 + a_5\sqrt[3]{5} + b_1\sqrt[3]{5}^2)\sqrt{5} = a_0 + a_2b^2 + a_4b^4 + a_3b^3 + a_5b^5 + b_1b^7 = a_0 + a_2b^2 + a_4b^4 + a_3b^3 + a_5b^5 + 5b_1b = a_0 + a_2b^2 + a_4b^4 + a_3b^3 + a_5b^5 + a_1b$.

Alternativ Lösung: Es gilt $b = \frac{\sqrt{5}}{\sqrt[3]{5}}$, da $\frac{\sqrt{5}}{\sqrt[3]{5}}$ reell und positiv ist, und $(\frac{\sqrt{5}}{\sqrt[3]{5}})^6 = \frac{\sqrt{5}^6}{\sqrt[3]{5}^6} = \frac{5^3}{5^2} = 5$. Also $b \in \mathbb{Q}(\sqrt{5}, \sqrt[3]{5})$. b ist eine Nullstelle des Polynoms $x^6 - 5$, das irreduzibel über $\mathbb{Q}$ ist aus Eisensteinskriterium. Also gilt $\text{MiPo}_{b/\mathbb{Q}} = x^6 - 5$ und $[\mathbb{Q}(b) : \mathbb{Q}] = 6$. Aber $\mathbb{Q}(b) \subseteq \mathbb{Q}(\sqrt{5}, \sqrt[3]{5})$, und $6 = [\mathbb{Q}(\sqrt{5}, \sqrt[3]{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{5}, \sqrt[3]{5}) : \mathbb{Q}(b)][\mathbb{Q}(b) : \mathbb{Q}] = 6[\mathbb{Q}(\sqrt{5}, \sqrt[3]{5}) : \mathbb{Q}(b)]$, also $[\mathbb{Q}(\sqrt{5}, \sqrt[3]{5}) : \mathbb{Q}(b)] = 1$ und $\mathbb{Q}(\sqrt{5}, \sqrt[3]{5}) = \mathbb{Q}(b)$. Daraus folgt, dass jede $x \in \mathbb{Q}(\sqrt{5}, \sqrt[3]{5}) = \mathbb{Q}(b)$ lässt sich als $\sum_{i=0}^5 a_i b^i$ mit $a_i \in \mathbb{Q}$ schreiben.

f) $\sqrt{5}$ und $\sqrt[3]{5}$ sind Nullstellen von f , also ist $\mathbb{Q}(\sqrt{5}, \sqrt[3]{5}) \subseteq L$. f lässt sich als $(x - \sqrt{5})(x + \sqrt{5})(x - \sqrt[3]{5})(x^2 - \sqrt[3]{5}x + \sqrt[3]{5}^2)$ in $\mathbb{Q}(\sqrt{5}, \sqrt[3]{5})$ faktorisieren. $(x^2 - \sqrt[3]{5}x + \sqrt[3]{5}^2)$ hat keine Nullstelle in $\mathbb{R}$, und hat auch keine Nullstelle in $\mathbb{Q}(\sqrt{5}, \sqrt[3]{5}) \subseteq \mathbb{R}$. Also ist $L = \mathbb{Q}(\sqrt{5}, \sqrt[3]{5}, a)$, wobei a eine Nullstelle von $(x^2 - \sqrt[3]{5}x + \sqrt[3]{5}^2)$ ist. Also hat $L/\mathbb{Q}(\sqrt{5}, \sqrt[3]{5})$ Grad 2, und $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{5}, \sqrt[3]{5})][\mathbb{Q}(\sqrt{5}, \sqrt[3]{5}) : \mathbb{Q}] = 2 \cdot 6 = 12$.

Aufgabe 5.

a) Es gilt $b_{\pm} = \frac{-4 \pm \sqrt{4^2 + 24}}{2} = -2 \pm \frac{\sqrt{40}}{2} = -2 \pm \sqrt{10}$, also nehmen wir $c = 10$.

b) Es gilt $f(a_1) = a_1^4 + 4a_1^2 - 6 = b_+^2 + 4b_+ - 6 = g(b_+) = 0$, und f ist irreduzibel über $\mathbb{Q}$ aus Eisensteinskriterium (mit $p = 2$), also ist f das Minimalpolynom von a_1 über $\mathbb{Q}$.

c) Es gilt $b_+ = a_1^2$, also $b_+ \in \mathbb{Q}(a_1)$ und $\mathbb{Q}(b_+) \subseteq \mathbb{Q}(a_1)$. Es gilt $[\mathbb{Q}(a_1) : \mathbb{Q}] = 4$ da $\text{MiPo}_{a_1/\mathbb{Q}} = f$ hat Grad 4, $[\mathbb{Q}(b_+) : \mathbb{Q}] = 2$ da $\text{MiPo}_{b_+/\mathbb{Q}} = g$ hat Grad 2. Daraus folgt $4 = [\mathbb{Q}(a_1) : \mathbb{Q}] = [\mathbb{Q}(a_1) : \mathbb{Q}(b_+)][\mathbb{Q}(b_+) : \mathbb{Q}] = [\mathbb{Q}(a_1) : \mathbb{Q}(b_+)] \cdot 2$, also $[\mathbb{Q}(a_1) : \mathbb{Q}(b_+)] = 2$.

d) Da $a_1 = -a_2$, gilt $a_1 \in \mathbb{Q}(a_2)$ und $a_2 \in \mathbb{Q}(a_1)$, also $\mathbb{Q}(a_1) = \mathbb{Q}(a_2)$.

Da $a_3 = -a_4$, gilt ähnlich $\mathbb{Q}(a_3) = \mathbb{Q}(a_4)$.

Da $\mathbb{Q}(a_1) \subseteq \mathbb{R}$ ist, aber $a_3 \notin \mathbb{R}$, gilt $\mathbb{Q}(a_1) \neq \mathbb{Q}(a_3)$.

e) Es gilt $f(a_2) = g(b_+) = 0$, $f(a_3) = g(b_-) = 0$, und $f(a_4) = g(b_-) = 0$. Da die a_i paarweise verschiedene sind, sind a_1, a_2, a_3, a_4 alle Nullstellen von f , und $L = \mathbb{Q}(a_1, a_2, a_3, a_4)$. Da $a_2 \in \mathbb{Q}(a_1)$ und $a_4 \in \mathbb{Q}(a_3)$ liegen, gilt $L = \mathbb{Q}(a_1, a_2, a_3, a_4) = \mathbb{Q}(a_1, a_3)$.

f) Es gilt $[\mathbb{Q}(a_1) : \mathbb{Q}(b_+)] = 2$, also betrachten wir die Körpererweiterung $\mathbb{Q}(a_1, a_3)/\mathbb{Q}(a_1)$. Es gilt $a_3 \notin \mathbb{Q}(a_1)$, also $[\mathbb{Q}(a_1, a_3)/\mathbb{Q}(a_1)] > 1$. Über $\mathbb{Q}(a_1)$ lässt sich f als $(x - a_1)(x + a_1)h$ faktorisieren, mit $h \in \mathbb{Q}(a_1)[x]$ der Grad 2, und $h(a_3) = 0$. Also $\text{MiPo}_{a_3/\mathbb{Q}(a_1)}$ teilt h , und sein Grad ist ≤ 2 ; daraus folgt $[\mathbb{Q}(a_1, a_3)/\mathbb{Q}(a_1)] \leq 2$ und $[\mathbb{Q}(a_1, a_3)/\mathbb{Q}(a_1)] = 2$. Schließlich gilt $[\mathbb{Q}(a_1, a_3)/\mathbb{Q}(b_+)] = [\mathbb{Q}(a_1, a_3)/\mathbb{Q}(a_1)][\mathbb{Q}(a_1)/\mathbb{Q}(b_+)] = 2 \cdot 2 = 4$.

g) Aus der Hauptsatz der Galois-Theorie folgt, dass $\text{Aut}(L/\mathbb{Q}(a_1))$ ein Normalteiler von $\text{Aut}(L/\mathbb{Q})$ genau dann ist, wenn $\mathbb{Q}(a_1)/\mathbb{Q}$ eine normale Körpererweiterung ist. Aber $\mathbb{Q}(a_1)/\mathbb{Q}$ ist nicht normale, da $\text{MiPo}_{a_1/\mathbb{Q}} = f$, und der Zerfällungskörper von f ist $L \supsetneq \mathbb{Q}(a_1)$.

Also hat $\text{Aut}(L/\mathbb{Q})$ eine Untergruppe, die nicht Normal ist, und das impliziert, dass $\text{Aut}(L/\mathbb{Q})$ nicht abelsch ist.