

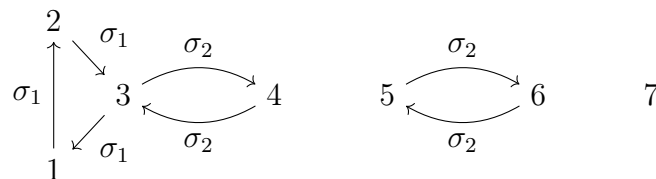
Algebra
Nachklausur
Lösungsvorschlag

Aufgabe 1.

- a)
 - Es gilt $0 = \frac{0}{6} \in H_1$.
 - Seien $a, b \in H_1$. Dann existieren $r, s \in \mathbb{Z}$ mit $a = \frac{r}{6}$ und $b = \frac{s}{6}$. Also ist $a + b = \frac{r+s}{6} \in H_1$.
 - Sei $a \in H_1$. Dann existiert $r \in \mathbb{Z}$ sodass $a = \frac{r}{6}$. Also ist $-a = \frac{-r}{6} \in H_1$.
- b) Es gilt $\frac{5}{6} \in H_1$, also $H_2 = \langle \frac{5}{6} \rangle \subseteq H_1$.
Es gilt $H_2 = \langle \frac{5}{6} \rangle = \{ \frac{5r}{6} \mid r \in \mathbb{Z} \}$. Insbesondere, $\frac{1}{6} \in H_1 \setminus H_2$, also $H_1 \not\subseteq H_2$.
- c) Es gilt $\langle \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \dots \rangle \subseteq \mathbb{Q}$. Sei nun $a \in \mathbb{Q}$, also existieren $r \in \mathbb{Z}$ und $s \in \mathbb{N}_{>0}$ mit $a = \frac{r}{s}$. Dann ist $a = r \frac{1}{s} \in \langle \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \dots \rangle$.
- d) Seien $r_1, \dots, r_k \in \mathbb{Q}$, also existieren $a_1, \dots, a_k \in \mathbb{Z}$ und $b_1, \dots, b_k \in \mathbb{N}_{>0}$ sodass $r_i = \frac{a_i}{b_i}$ für $1 \leq i \leq k$. Wir setzen $n = \prod_{i=1}^k b_i$. Dann gilt $r_i = \frac{a_i}{b_i} = a_i \prod_{j \neq i} b_j \frac{1}{n}$, das heißt, $r_i \in \langle \frac{1}{n} \rangle$ für $1 \leq i \leq k$, und $\langle r_1, \dots, r_k \rangle \subseteq \langle \frac{1}{n} \rangle$.
- e) Es gilt $\frac{3}{2} = 9\frac{1}{6} \in \langle \frac{1}{6} \rangle$ und $\frac{4}{3} = 8\frac{1}{6} \in \langle \frac{1}{6} \rangle$, also $\langle \frac{3}{2}, \frac{4}{3} \rangle \subseteq \langle \frac{1}{6} \rangle$.
Es gilt auch $\frac{1}{6} = \frac{9}{6} - \frac{8}{6} = \frac{3}{2} - \frac{4}{3} \in \langle \frac{3}{2}, \frac{4}{3} \rangle$, also $\langle \frac{3}{2}, \frac{4}{3} \rangle \subseteq \langle \frac{1}{6} \rangle$.

Aufgabe 2.

- a) Es gilt $\sigma_1 \circ \sigma_2 = \widehat{123456}$.
- b) Es gilt $\sigma_1 = \widehat{1223} \in A_7$ und $\sigma_2 = \widehat{3456} \in A_7$, also $G = \langle \sigma_1, \sigma_2 \rangle \subseteq A_7$.
- c) Es gilt $\sigma_2 \sigma_1 \sigma_2^{-1} = \sigma_2 \widehat{123} \sigma_2^{-1} = \widehat{\sigma_2(1)\sigma_2(2)\sigma_2(3)} = \widehat{124} \notin \langle \sigma_1 \rangle$, also $\sigma_2 \langle \sigma_1 \rangle \sigma_2^{-1} \neq \langle \sigma_1 \rangle$ und $\langle \sigma_1 \rangle$ ist nicht normal in G .
- d) Die Wirkung von G auf $\{1, 2, \dots, 7\}$ ist gegeben durch:



Also $G2 = \{1, 2, 3, 4\}$.

- e) Es gilt $G7 = \{7\}$, also $\text{Stab}_G(7) = G$.
- f) Es gilt $\sigma_2 \sigma_1 \sigma_2^{-1} = \widehat{124} \in \S \{1, a, \dots, a^4, \sqrt{2}, a\sqrt{2}, \dots, a^4\sqrt{2}\} \text{ tab}_G(5) \notin \langle \sigma_1 \rangle$ aus (c).

Aufgabe 3.

a) Es gilt $\mathfrak{a}_2 \subsetneq \mathfrak{a}_3 \subsetneq \mathfrak{a}_1$, da

- $xy \in (x)$, also $\mathfrak{a}_2 \subseteq \mathfrak{a}_3$; und $x \notin (xy)$, da kein $z \in \mathbb{Q}[x, y]$ existiert, mit $xyz = x$, weil y nicht invertierbar in $\mathbb{Q}[x, y]$ ist. Also $x \in \mathfrak{a}_3 \setminus \mathfrak{a}_2$ und $\mathfrak{a}_2 \subsetneq \mathfrak{a}_3$.
- $x \in (x, y)$, also $\mathfrak{a}_3 \subseteq \mathfrak{a}_1$; und $y \notin (x)$, da kein $z \in \mathbb{Q}[x, y]$ existiert, mit $xz = y$, weil x und y nicht equivalent zu einanders in $\mathbb{Q}[x, y]$ sind. Also $y \in \mathfrak{a}_1 \setminus \mathfrak{a}_3$ und $\mathfrak{a}_3 \subsetneq \mathfrak{a}_1$.

b) Es gilt $x \notin \mathfrak{a}_2$ (aus (a)) und ähnlich $y \notin \mathfrak{a}_2$, also sowohl $\bar{x} \neq 0 \in \mathbb{Q}[x, y]/\mathfrak{a}_2$ als $\bar{y} \neq 0$. Aber $xy \in \mathfrak{a}_2$, also $\bar{x}\bar{y} = \overline{xy} = 0 \in \mathbb{Q}[x, y]/\mathfrak{a}_2$.

c) Sei $f: \mathbb{Q}[x, y]/\mathfrak{a}_2 \rightarrow \mathbb{Q}[y]$ ein Ringhomomorphismus mit $f(\bar{y}) = y$. Dann gilt sowohl $f(\bar{x}\bar{y}) = f(0) = 0$ als $f(\bar{x}\bar{y}) = f(\bar{x})f(\bar{y}) = f(\bar{x})y$, also $f(\bar{x})y = 0$. Da $\mathbb{Q}[x, y]$ kein Nullteiler besitzt (er ist ein Integritätsbereich), muss entweder $f(\bar{x}) = 0$ oder $y = 0$ gelten. Aus $y \neq 0$ folgt, dass $f(\bar{x}) = 0$.

d) Wir betrachten als erstes Elemente der Form $ax^i y^j \in \mathbb{Q}[x, y]$. Wenn sowohl i als j nicht null sind, dann gilt $ax^i y^j = xy \cdot ax^{i-1} y^{j-1}$, also $ax^i y^j \in \mathfrak{a}_2$ und $\overline{ax^i y^j} = 0 \in \mathbb{Q}[x, y]/\mathfrak{a}_2$.

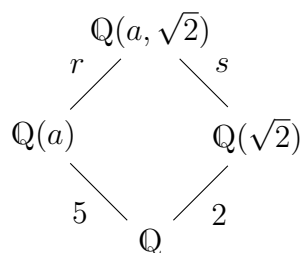
Sei nun $T = \sum_{i,j \leq n} a_{ij} x^i y^j \in \mathbb{Q}[x, y]$. Dann ist $\bar{T} = \sum_{i,j \leq n} \overline{a_{ij} x^i y^j} \in \mathbb{Q}[x, y]/\mathfrak{a}_2$. Aus unsere Berechnung folgt, dass $\bar{T} = \sum_{j \leq n} \overline{a_{0j} y^j} + \sum_{0 < i \leq n} \overline{a_{i0} x^i}$. Wir setzen $f = \sum_{0 < i \leq n} a_{i0} x^i$ und $g = \sum_{j \leq n} a_{0j} y^j$, dann ist $\bar{T} = \bar{f} + \bar{g}$.

Aufgabe 4.

a) Wir benutzen Eisensteinskriterion mit der Prim 3: $3 \nmid 1$, $3 \mid 6$, $3 \mid 9$, $3 \mid 12$ und $3^2 \nmid 12$; also f ist irreduzibel über $\mathbb{Q}$.

b) Da $\deg(f) = 5$, gilt $[\mathbb{Q}(a) : \mathbb{Q}] = 5$. Wenn $\sqrt{2} \in \mathbb{Q}(a)$ liegt, gilt $5 = [\mathbb{Q}(a) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2[\mathbb{Q}(a) : \mathbb{Q}(\sqrt{2})]$. Aber $2 \nmid 5$, also $\sqrt{2} \notin \mathbb{Q}(a)$.

c) Wir betrachten die Folgende Karo:



Wir haben $[\mathbb{Q}(a) : \mathbb{Q}] = 5$ aus (a), $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ offensichtlich, und wir setzen $[\mathbb{Q}(a, \sqrt{2}) : \mathbb{Q}(a)] = r$ und $[\mathbb{Q}(a, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = s$. Aus (b) folgt, dass die Erweiterung $\mathbb{Q}(a) \subseteq \mathbb{Q}(a, \sqrt{2})$ nicht triviale ist, also $r > 1$. Da $\sqrt{2}$ eine Nullstelle von $x^2 - 2$ ist, gilt $r \leq 2$, also $r = 2$. Daraus folgt $[\mathbb{Q}(a, \sqrt{2}) : \mathbb{Q}] = 10 = 2s$, also $[\mathbb{Q}(a, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = s = 5$.

d) Da $[\mathbb{Q}(a) : \mathbb{Q}] = 5$, ist $\{1, a, a^2, a^3, a^4\}$ eine $\mathbb{Q}$ -Basis von $\mathbb{Q}(a)$. Insbesondere sind sie linear unabhängig über $\mathbb{Q}$ und sie sind maximale solche.

- e) Es folgt aus (c), dass $[\mathbb{Q}(a, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = 5$. Eine $\mathbb{Q}(\sqrt{2})$ -Basis von $\mathbb{Q}(a, \sqrt{2})$ ist $\{1, a, a^2, a^3, a^4\}$. Sei $x \in \mathbb{Q}(a, \sqrt{2})$, dann existieren $b_0, \dots, b_4 \in \mathbb{Q}(\sqrt{2})$ mit $x = b_0 + b_1 a + \dots + b_4 a^4$.

Da $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, ist $\{1, \sqrt{2}\}$ eine $\mathbb{Q}$ -Basis von $\mathbb{Q}(\sqrt{2})$. Da $b_i \in \mathbb{Q}(\sqrt{2})$ ist, existieren $c_i, d_i \in \mathbb{Q}$ mit $b_i = c_i + d_i \sqrt{2}$.

Daraus folgt, dass $x = b_0 + \dots + b_4 a^4 = c_0 + d_0 \sqrt{2} + c_1 a + d_1 a \sqrt{2} + \dots + c_4 a^4 + d_4 a^4 \sqrt{2}$. Das heißt, $\{1, a, \dots, a^4, \sqrt{2}, a\sqrt{2}, \dots, a^4 \sqrt{2}\}$ ist eine Erzeugendefamilie von $\mathbb{Q}(a, \sqrt{2})$ über $\mathbb{Q}$. Da $[\mathbb{Q}(a, \sqrt{2}) : \mathbb{Q}] = 10$ und $\#\{1, a, \dots, a^4, \sqrt{2}, a\sqrt{2}, \dots, a^4 \sqrt{2}\} = 10$, folgt dass $\{1, a, \dots, a^4, \sqrt{2}, a\sqrt{2}, \dots, a^4 \sqrt{2}\}$ eine $\mathbb{Q}$ -Basis von $\mathbb{Q}(a, \sqrt{2})$ ist, insbesondere, linear unabhängig.

Aufgabe 5.

- a) Es gilt $\zeta_{p^2}^{p^2} - 1 = 0$, also $f(\zeta_{p^2})(\zeta_{p^2}^p - 1) = 0$. Aber $\zeta_{p^2}^p \neq 1$, also $f(\zeta_{p^2}) = 0$. Da f irreduzibel ist, ist f das Minimalpolynom von ζ_{p^2} .
- b) Sei $k \in \mathbb{N}$ mit $1 \leq k \leq p^2$. Dann ist $\zeta_{p^2}^k = 1$. Also das Polynom $x^{p^2} - 1$ zerfällt (in $\mathbb{C}$) als $(x - \zeta_{p^2})(x - \zeta_{p^2}^2) \dots (x - \zeta_{p^2}^{p^2})$. Da $\zeta_{p^2}^k \in \mathbb{Q}(\zeta_{p^2})$ liegt, zerfällt $x^{p^2} - 1$ in $\mathbb{Q}(\zeta_{p^2})$. Da $f \mid x^{p^2} - 1$, zerfällt auch f in $\mathbb{Q}(\zeta_{p^2})$.
- c) Für alle solche r ist $\zeta_{p^2}^r$ eine Nullstelle von $x^{p^2} - 1$. Aber $\zeta_{p^2}^r$ ist eine Nullstelle von $x^p - 1$ gdw. $p \mid r$, also ist $\zeta_{p^2}^r$ eine Nullstelle von f gdw. $p \nmid r$ gdw. $r \in \{0, 1, \dots, p^2 - 1\} \setminus \{0, p, \dots, p(p-1)\}$.
- d) Sei $a = \zeta_p = \zeta_{p^2}^p$, dann gilt $a \in L$ und $[\mathbb{Q}(a) : \mathbb{Q}] = p - 1$ (aus der Vorlesung).
- e) Da $L/\mathbb{Q}$ Normal ist, gilt $\#\text{Aut}(L/\mathbb{Q}) = [L : \mathbb{Q}] = p(p-1)$. Sei $K' \subseteq L$ mit $[K' : \mathbb{Q}] = p - 1$. Dann gilt $\#\text{Aut}(L/K') = [L : K'] = \frac{[L:\mathbb{Q}]}{[K':\mathbb{Q}]} = \frac{p(p-1)}{p-1} = p$. Aus Galois-Theorie folgt, dass $\text{Aut}(L/K')$ eine Untergruppe von $\text{Aut}(L/\mathbb{Q})$ ist. Wir betrachten die Sylow-Sätze mit p : die Sylow- p -Untergruppe von $\text{Aut}(L/\mathbb{Q})$ sind der Ordnung p , also ist $\text{Aut}(L/K')$ eine Sylow- p -Untergruppe. Die Anzahl der Sylow- p -Untergruppen s_p erfüllt $s_p \mid p-1$ und $s_p \equiv 1 \pmod{p}$, also $s_p = 1$ und $\text{Aut}(L/K')$ ist die Einzige Sylow- p -Untergruppe.

Daraus folgt, dass $\text{Aut}(L/K') = \text{Aut}(L/K)$ ist, und aus der Hauptsatz der Galois-Theorie folgt, dass $K = K'$.