**Universität Konstanz** Christoph Hanselka
**Fachbereich Mathematik und Statistik** Markus Schweighofer
**16. März 2015** Wintersemester 2014/2015

---

Klausur zur Einführung in die Algebra, Lösungsvorschlag

---

**Aufgabe 1 (10 Punkte).** Betrachte die Gruppe $\mathrm{GL}_2(\mathbb{F}_2)$ aller invertierbaren $2 \times 2$-Matrizen über dem zweielementigen Körper $\mathbb{F}_2$.

(a) Gib alle Untergruppen von $\mathrm{GL}_2(\mathbb{F}_2)$ explizit an! Führe dabei jede nur einmal auf! Eine Begründung ist nicht erforderlich. Notation aus der Vorlesung darf natürlich benutzt werden. (5 Punkte)

(b) Argumentiere, warum es außer den in (a) aufgeführten Untergruppen keine weiteren mehr gibt. (5 Punkte)

**Lösungsvorschlag.** (a) $\mathrm{GL}_2(\mathbb{F}_2)$, $\{1\}$, $\ntriangleright_2(\mathbb{F}_2)$, $\ntriangleleft_2(\mathbb{F}_2)$, $\left\{1, \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)\right\}$, $\left\{1, \left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)\right\}$

(b) Wegen $\mathrm{GL}_2(\mathbb{F}_2) = \left\{1, \left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)\right\}$ gilt $\#\mathrm{GL}_2(\mathbb{F}_2) = 6 = 2 \cdot 3$. Daher gibt es neben den trivialen Untergruppen $\mathrm{GL}_2(\mathbb{F}_2)$ und $\{1\}$ nach dem Satz von Lagrange nur Untergruppen der Ordnung 2 und der Ordnung 3. Zudem sind hier die nichttrivialen Untergruppen alles Sylowgruppen. Für die Anzahl $n_2$ der 2-Sylowgruppen gilt $n_2 \equiv_{(2)} 1$ und $n_2 | 6$, also $n_2 \in \{1, 3\}$. Daher gibt es höchstens 3 Untergruppen der Ordnung 2 und in (a) sind schon 3 solche aufgeführt. Für die Anzahl $n_3$ der 3-Sylowgruppen gilt $n_3 \equiv_{(3)} 1$ und $n_3 | 6$, also $n_3 = 1$. Daher gibt es höchstens eine Untergruppe der Ordnung 3 und in (a) ist eine solche aufgeführt.

**Aufgabe 2 (20 Punkte).** Sei $G$ eine Gruppe der Ordnung 14. Zeige:

(a) $G$ besitzt genau eine Untergruppe $N$ der Ordnung 7. (3 Punkte)

(b) $N$ ist ein Normalteiler von $G$ (in Zeichen: $N \lhd G$). (1 Punkt)

(c) $G$ besitzt eine Untergruppe $H$ der Ordnung 2. (Fixiere im folgenden eine solche.) (2 Punkte)

(d) $G$ ist semidirektes Produkt von $N$ und $H$ (in Zeichen: $G = N \rtimes H$). (2 Punkte)

(e) $H \cong C_2$ und $N \cong C_7$ (2 Punkte)

(f) Bezeichnet $h$ das eindeutig bestimmte Element von $H$ mit $H = \{1, h\}$, so gibt es ein $k \in \{1, \ldots, 6\}$ derart, dass $hxh^{-1} = x^k$ für alle $x \in N$. (2 Punkte)

(g) $x = x^{k^2}$ für alle $x \in N$ (2 Punkte)

(h) $k \in \{1, 6\}$ (2 Punkte)

(i) Es gibt bis auf Isomorphie höchstens zwei Gruppen der Ordnung 14. (2 Punkte)

(j) $G \cong C_{14}$ oder $G \cong D_7$ (2 Punkte)

**Lösungsvorschlag.** (a) Wegen $14 = 7 \cdot 2$ ist jede Untergruppe der Ordnung 7 sogar eine 7-Sylowgruppe von $G$. Für die Anzahl $n_7$ der 7-Sylowgruppen von $G$ gilt $n_7 \equiv_{(7)} 1$ und $n_7 | 14$, also $n_7 = 1$.

(b) Da $N$ die einzige Untergruppe der Ordnung 7 von $G$ ist, ist $N$ offenbar eine charakteristische Untergruppe von $G$ und damit insbesondere ein Normalteiler von $G$.

(c) $G$ besitzt mindestens eine 2-Sylowgruppe und diese hat wegen $\#G = 14$ die Ordnung 2.

(d) Da $N$ ein Normalteiler und $H$ eine Untergruppe von $G$ ist, wissen wir aus der Vorlesung, dass $NH = \{ab \mid a \in N, b \in H\}$ eine Untergruppe von $G$ ist. Es ist $NH = G$ und $N \cap H = \{1\}$ zu zeigen. Ersteres folgt daraus, dass nach dem Satz von Lagrange die Gruppenordnung von $NH$ sowohl ein Vielfaches sowohl von 2 als auch von 7 ist (denn $N \leq NH$ und $H \leq NH$). Wäre $N \cap H \neq \{1\}$, so wäre $H \subseteq N$ (denn $H$ hat ausser dem neutralen Element, welches auch in $N$ enthalten ist, nur ein einziges anderes Element) im Widerspruch zu $NH = G \neq N$.

(e) Es reicht zu zeigen, dass $H$ und $N$ zyklisch sind. Dies folgt aus der folgenden allgemeinen Tatsache, die sofort aus dem Satz von Lagrange folgt: Eine Gruppe von Primzahlordnung wird von jedem Element $\neq 1$ erzeugt.

(f) Wähle gemäß (e) ein $y \in N$ mit $N = \{1, y, y^2, \ldots, y^6\}$. Da $N$ ein Normalteiler von $G$ ist, können wir $k \in \{0, \ldots, 6\}$ wählen mit $hyh^{-1} = y^k$. Wäre $k = 0$, so wäre $y = h^{-1}h = 1$, was absurd ist. Also ist $k \in \{1, \ldots, 6\}$. Es folgt $hy^\ell h^{-1} = (hyh^{-1})^\ell = (y^k)^\ell = y^{k\ell} = (y^\ell)^k$ für $\ell \in \{0, \ldots, 6\}$ (sogar für $\ell \in \mathbb{Z}$) und daher $hxh^{-1} = x^k$ für alle $x \in N$.

(g) Wegen $\#H = 2$ muss $h^2 = 1$ gelten. Wegen (f) gilt daher

$$x = h^2xh^{-2} = h(hxh^{-1})h^{-1} = hx^kh^{-1} = (x^k)^k = x^{k^2}$$

für alle $x \in N$.

(h) Wähle $x \in N \setminus \{1\}$ fest. Nach (g) gilt $x^{k^2-1} = 1$. Da $x$ die Ordnung 7 hat und nach Teilaufgabe (g) $x^{k^2-1} = 1$ gilt, muss 7 ein Teiler von $k^2 - 1$ sein. Zusammen mit $k \in \{1, \ldots, 6\}$ sieht man daraus leicht $k \in \{1, 6\}$.

(i) Wähle wieder $y \in N \setminus \{1\}$ fest. Dann gilt $N = \{y^0, \ldots, y^6\}$ mit $\#N = 7$, $H = \{1, h\}$ mit $\#H = 2$ und $G \overset{(d)}{=} NH = \{y^0, \ldots, y^6, y^0h, \ldots, y^6h\}$ mit $\#G = 14$. Nun kann man die Multiplikationstabelle leicht ausfüllen. In Termini von $y$ und $h$ wird diese nur noch von $k$ aus (h) abhängen, denn $y^iy^j = y^{i+j}$, $y^i(y^jh) = y^{i+j}h$, $(y^ih)y^j = y^i(hy^jh^{-1})h = y^i(y^j)^kh = y^{i+jk}h$ und $(y^ih)(y^jh) = y^i(hy^jh^{-1}) = y^i(y^j)^k = y^{i+jk}$ für alle $i, j \in \{0, \ldots, 6\}$. Die Multiplikationstabelle von $G$ kann also wegen (h) nur zwei mögliche Gestalten

annehmen. Daher kann es bis auf Isomorphie höchstens zwei Gruppen der Ordnung 14 geben.

(j) $C_{14}$ und $D_7$ sind Gruppen der Ordnung 14, die nicht isomorph sind (denn $C_{14}$ ist abelsch und $D_7$ nicht). Nach (i) muss also $G \cong C_{14}$ oder $G \cong D_7$ gelten.

**Aufgabe 3 (12 Punkte).** Betrachte das Polynom $f := 2X^5 - 6X + 6 \in \mathbb{Z}[X]$. In welchen der folgenden Ringe ist $f$ irreduzibel? Begründe jeweils Deine Antwort.

(a) $\mathbb{Z}[X]$ (2 Punkte)

(b) $(S^{-1}\mathbb{Z})[X]$ mit $S := \{2^n \mid n \in \mathbb{N}_0\}$ (4 Punkte)

(c) $\mathbb{Q}[X]$ (4 Punkte)

(d) $\mathbb{R}[X]$ (1 Punkt)

(e) $\mathbb{C}[X]$ (1 Punkt)

**Lösungsvorschlag.** (a) $f = 2(X^5 - 3X + 3) \in \mathbb{Z}[X]$ mit $2 \in \mathbb{Z}[X] \setminus \mathbb{Z}[X]^\times$ und $X^5 - 3X + 3 \in \mathbb{Z}[X] \setminus \mathbb{Z}[X]^\times$ ist eine Zerlegung von $f$ in zwei Nichteinheiten von $\mathbb{Z}[X]$ (beachte $\mathbb{Z}[X]^\times = \mathbb{Z}^\times = \{-1, 1\}$). Daher ist $f$ nicht irreduzibel in $\mathbb{Z}[X]$.

(c) Da 2 eine Einheit in $S^{-1}Z[X]$ ist, untersuchen wir das Polynom $g := X^5 - 3X + 3$ anstatt von $f$. Dieses Polynom $g$ ist nach dem Kriterium von Eisenstein angewandt auf das Primelement 3 von $\mathbb{Z}$ irreduzibel über $\mathbb{Z}$ und dem Quotientenkörper $\mathbb{Q}$ von $\mathbb{Z}$, also in $\mathbb{Q}[X]$. Daher ist $g$ und damit auch $f$ irreduzibel in $\mathbb{Q}[X]$, was wir in Teilaufgabe (b) benutzen werden.

(b) Wir behaupten, dass $f$ auch irreduzibel im Unterring $(S^{-1}\mathbb{Z})[X]$ von $\mathbb{Q}[X]$ ist. Hierzu ist zunächst zu beachten, dass $f$ als Polynom vom Grad $\geq 1$ keine Einheit in $(S^{-1}\mathbb{Z})[X]$ ist. Da 2 auch eine Einheit in $S^{-1}\mathbb{Z}[X]$ ist, reicht es wieder das Polynom $g = X^5 - 3X + 3$ zu betrachten. Seien also $p, q \in (S^{-1}\mathbb{Z})[X]$ mit $g = pq$. Zu zeigen ist $p \in (S^{-1}\mathbb{Z})[X]^\times$ oder $q \in (S^{-1}\mathbb{Z})[X]^\times$. Dann gilt nach (c), dass mindestens eines der beiden Polynome $p$ und $q$ den Grad 0 hat (beachte $\mathbb{Q}[X]^\times = \mathbb{Q}^\times$). Œ habe $p$ den Grad 0, also $p \in S^{-1}\mathbb{Z}$. Es teilt nun $p$ im Ring $S^{-1}\mathbb{Z}$ jeden Koeffizienten von $g$, insbesondere auch dessen Leitkoeffizienten 1. Das bedeutet gerade, dass $p$ eine Einheit ist.

*Bemerkung:* Es lässt sich alternativ auch zeigen, dass $S^{-1}\mathbb{Z}$ ein faktorieller Ring ist, in welchem 3 ein Primelement ist, was wir aber hier nicht weiter ausführen. Damit lässt sich das Kriterium von Eisenstein auch unmittelbar auf $g$ und $S^{-1}\mathbb{Z}$ anwenden.

(d) Offensichtlich gilt $\lim_{x\to\infty} f(x) = \infty$ und $\lim_{x\to-\infty} f(x) = -\infty$. Insbesondere nimmt $f$ positive und negative Werte auf $\mathbb{R}$ an. Nach dem Zwischenwertsatz aus der Analysis hat $f$ eine Nullstelle in $\mathbb{R}$. Da $f$ ausserdem Grad $\geq 2$ hat, ist $f$ reduzibel in $\mathbb{R}[X]$.

(e) Nach dem Fundamentalsatz der Algebra hat $f$ eine Nullstelle in $\mathbb{C}$. Da $f$ ausserdem Grad $\geq 2$ hat, ist $f$ reduzibel in $\mathbb{C}[X]$.

**Aufgabe 5 (6 Punkte + 8 Bonuspunkte).** Welche der folgenden drei Ideale in $\mathbb{C}[X,Y]$ sind Primideale? Welche sind maximale Ideale?

$$I := (XY), \qquad J := (X+Y), \qquad K := (X,Y)$$

Eine Begründung ist nicht erforderlich. Bei vollständiger Begründung gibt es aber bis zu 8 Bonuspunkten.

**Lösungsvorschlag.** $I$ ist nicht prim und daher auch nicht maximal, $J$ ist prim aber nicht maximal, $K$ ist maximal und daher auch prim.

Zum Bonusteil:

$I$ ein Primideal von $\mathbb{R}[X,Y]$ genau dann, wenn $XY$ ein Primelement in $\mathbb{R}[X,Y]$. Da $X, Y \notin \mathbb{R}^\times = \mathbb{R}[X,Y]^\times$ ist aber $XY$ nicht irreduzibel in $\mathbb{R}[X,Y]$ und damit insbesondere nicht prim (beachte $XY \neq 0$). Also ist $I$ kein Primideal in $\mathbb{R}[X,Y]$.

$J$ ist ein Primideal genau dann, wenn $\mathbb{R}[X,Y]/J$ ein Integritätsring ist. Dazu reicht es zu zeigen, dass $\mathbb{R}[X,Y]/J \cong \mathbb{R}[X]$, denn $\mathbb{R}[X]$ ist ein Integritätsring. Wir betrachten dazu den Einsetzungshomomorphismus $\varphi\colon \mathbb{R}[X,Y] \to \mathbb{R}[X],\ p \mapsto p(X,-X)$. Wegen $\varphi(p) = p$ für alle $p \in \mathbb{R}[X]$ ist $\varphi$ surjektiv. Wegen $\varphi(X+Y) = X + (-X) = 0$ liegt $J$ im Kern von $\varphi$. Ist $p \in \ker\varphi$, so gilt $p \equiv_J p(X,-X) = \varphi(p) = 0$ und daher $p \in J$. Also gilt auch $\ker\varphi \subseteq J$ und daher $\ker\varphi = J$. Der Isomorphiesatz angewandt auf $\varphi$ liefert jetzt einen Ringisomorphismus von $\mathbb{R}[X,Y]/J$ nach $\mathbb{R}[X]$.

$J$ ist ein maximales Ideal genau dann, wenn $\mathbb{R}[X,Y]/K$ ein Körper ist. Dazu zeigen wir $\mathbb{R}[X,Y]/K \cong \mathbb{R}$. Wir betrachten dazu den Einsetzungshomomorphismus $\varphi\colon \mathbb{R}[X,Y] \to \mathbb{R},\ p \mapsto p(0,0)$. Offensichtlich ist $\varphi$ surjektiv und $K$ liegt im Kern von $\varphi$. Ist $p \in \ker\varphi$, so gilt $p \equiv_K p(0,0) = \varphi(p) = 0$ und daher $p \in K$. Also gilt auch $\ker\varphi \subseteq K$ und daher $\ker\varphi = K$. Der Isomorphiesatz angewandt auf $\varphi$ liefert jetzt einen Ringisomorphismus von $\mathbb{R}[X,Y]/K$ nach $\mathbb{R}$.

**Aufgabe 6 (30 Punkte).** Betrachte die reelle Zahl $x := \sqrt{2+\sqrt{2}}$ und den Körper $L := \mathbb{Q}(x)$.

(a) Finde ein normiertes Polynom $f \in \mathbb{Q}[X]$ vom Grad 4 mit $f(x) = 0$. (2 Punkte)

(b) Zeige, dass $f$ aus (a) irreduzibel in $\mathbb{Q}[X]$ ist. (3 Punkte)

(c) Begründe, warum es genau ein $f$ wie in (a) gibt. (2 Punkte)

(d) Bestimme alle vier verschiedenen Nullstellen $a_1, a_2, a_3, a_4$ von $f$ in $\mathbb{C}$. (3 Punkte)

(e) Zeige, dass $L$ der Zerfällungskörper von $f$ über $\mathbb{Q}$ ist. (3 Punkte)

*Hinweis:* Betrachte Produkte $a_i a_j$.

(f) Begründe, warum $L|\mathbb{Q}$ eine Galoiserweiterung ist. (2 Punkte)

(g) Begründe, warum es für jedes $i \in \{1,\dots,4\}$ genau ein $\varphi_i \in \mathrm{Aut}(L|\mathbb{Q})$ gibt mit $\varphi_i(a_1) = a_i$. (3 Punkte)

(h) Zeige $\mathrm{Aut}(L|\mathbb{Q}) = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$. (2 Punkte)

(i) Berechne $\varphi_i(\sqrt{2})$ für jedes $i \in \{1,2,3,4\}$. (2 Punkte)

*Hinweis:* Betrachte $\varphi_i(a_1^2)$.

(j) Berechne $\varphi_i(a_j)$ für alle $i, j \in \{1,2,3,4\}$. (4 Punkte)

*Hinweis:* Es kann dabei helfen, gewisse $\varphi_i(a_j a_k)$ zu betrachten.

(k) Zeige $\mathrm{Aut}(L|\mathbb{Q}) \cong C_4$. (2 Punkte)

(l) Bestimme alle Zwischenkörper von $L|\mathbb{Q}$. (2 Punkte)

**Lösungsvorschlag.** (a) Für $f := X^4 - 4X^2 + 2 \in \mathbb{Q}[X]$ gilt

$$\begin{aligned} f(x) &= \left(\sqrt{2+\sqrt{2}}\right)^4 - 4\left(\sqrt{2+\sqrt{2}}\right)^2 + 2 \\ &= (2+\sqrt{2})^2 - 4(2+\sqrt{2}) + 2 \\ &= 4 + 4\sqrt{2} + 2 - 8 - 4\sqrt{2} + 2 = 0. \end{aligned}$$

(b) Es ist $\mathbb{Z}$ ein faktorieller Ring, $f$ primitiv in $\mathbb{Z}[X]$ (sogar normiert) und 2 ein Primelement in $\mathbb{Z}$, welches alle Nichtleitkoeffizienten von $f$ teilt und dessen Quadrat den konstanten Koeffizienten von $f$ nicht teilt. Nach dem Kriterium von Eisenstein ist daher $f$ irreduzibel in ($\mathbb{Z}[X]$ und) $\mathbb{Q}[X]$.

(c) Da $f$ normiert und irreduzibel ist, ist $f$ das Minimalpolynom von $x$. Also hat nach (a) das Minimalpolynom von $x$ über $\mathbb{Q}$ den Grad 4. Jedes Polynom wie in (a) ist damit aber schon das Minimalpolynom von $x$ über $\mathbb{Q}$.

(d) Setze

$$a_1 := x = \sqrt{2+\sqrt{2}}, \quad a_2 := -\sqrt{2+\sqrt{2}}, \quad a_3 := \sqrt{2-\sqrt{2}} \quad \text{und} \quad a_4 := -\sqrt{2-\sqrt{2}}.$$

Man sieht sofort $a_2 < a_4 < 0 < a_3 < a_1$. Insbesondere sind $a_1, a_2, a_3, a_4$ paarweise verschieden. Durch ähnliche Rechnungen wie in (a) sieht man sofort $f(a_1) = f(a_2) = f(a_3) = f(a_4) = 0$.

(e) Es gilt $\sqrt{2} = x^2 - 2 \in \mathbb{Q}(x)$, $xa_3 = a_1 a_3 = \sqrt{2} \in \mathbb{Q}(x)$ und daher $a_3 = \frac{\sqrt{2}}{x} \in \mathbb{Q}(x)$. Damit gilt auch $a_2 = -x \in \mathbb{Q}(x)$ und $a_4 = -a_3 \in \mathbb{Q}(x)$. Also wird $\mathbb{Q}(x) = \mathbb{Q}(a_1, a_2, a_3, a_4)$ über $\mathbb{Q}$ von den Nullstellen von $f$ in $\mathbb{C}$ erzeugt. Damit ist $\mathbb{Q}(x)$ der Zerfällungskörper von $f$ über $\mathbb{Q}$.

(f) Als Zerfällungskörper eines Polynoms aus $\mathbb{Q}[X]$ ist $\mathbb{Q}(x)|\mathbb{Q}$ eine normale Körpererweiterung. Ferner ist diese Körpererweiterung natürlich separabel, da $\mathbb{Q}$ als Körper der Charakteristik 0 vollkommen ist.

(g) Betrachte $\mathbb{Q}(x)$ als Teilkörper des algebraischen Abschlusses $\overline{\mathbb{Q}}$ von $\mathbb{Q}$. Da $a_1, a_2, a_3, a_4$ alle dasselbe Minimalpolynom über $\mathbb{Q}$ haben, sind sie über $\mathbb{Q}$ konjugiert, das heißt es gibt für jedes $i \in \{1,2,3,4\}$ ein $\varphi \in \mathrm{Aut}(\overline{\mathbb{Q}}|\mathbb{Q})$ mit $\varphi(a_i) = a_j$. Nach (f) ist aber $\mathbb{Q}(x)|\mathbb{Q}$ normal, das heißt $\varphi(\mathbb{Q}(x)) = \mathbb{Q}(x)$ für alle $\varphi \in \mathrm{Aut}(\overline{\mathbb{Q}}|\mathbb{Q})$. Daher gibt für jedes $i \in \{1,2,3,4\}$ ein $\varphi \in \mathrm{Aut}(\mathbb{Q}(x)|\mathbb{Q})$ mit $\varphi(a_i) = a_j$. Es reicht daher zu zeigen, dass ein Automorphismus $\varphi$ der Körpererweiterung $\mathbb{Q}(x)|\mathbb{Q}$ schon durch $\varphi(x)$ bestimmt ist. Dies ist klar, denn sind $\varphi, \psi \in \mathrm{Aut}(\mathbb{Q}(x)|\mathbb{Q})$ mit $\varphi(x) = \psi(x)$, so liegt $x$ im Zwischenkörper $F := \{a \in \mathbb{Q}(x) \mid \varphi(a) = \psi(a)\}$ von $\mathbb{Q}(x)|\mathbb{Q}$, das heißt es gilt $F = \mathbb{Q}(x)$, also $\varphi = \psi$.

(h) „$\supseteq$“ ist trivial. Zu „$\subseteq$“: Sei $\varphi \in \mathrm{Aut}(L|\mathbb{Q})$. Mit $x$ ist dann auch $\varphi(x)$ eine Nullstelle von $f$. Daher gibt es ein $i \in \{1,2,3,4\}$ mit $\varphi(a_1) = a_i$. Dann gilt $\varphi = \varphi_i \in \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$.

(i) Es gilt $2 + \varphi_i(\sqrt{2}) = \varphi_i(2 + \sqrt{2}) = \varphi_i(a_1^2) = \varphi_i(a_1)^2 = a_i^2$ und daher $\varphi_i(\sqrt{2}) = a_i^2 - 2$. Also $\varphi_1(\sqrt{2}) = \sqrt{2}$, $\varphi_2(\sqrt{2}) = \sqrt{2}$, $\varphi_3(\sqrt{2}) = -\sqrt{2}$ und $\varphi_4(\sqrt{2}) = -\sqrt{2}$.

(j) Es gilt $a_3\varphi_3(a_1) = \varphi_3(a_1)^2 = \varphi_3(a_1^2) = \varphi_3(2 + \sqrt{2}) = 2 + \varphi_3(\sqrt{2}) \overset{\text{(i)}}{=} 2 - \sqrt{2}$ und daher $\varphi_3(a_1) = \frac{2-\sqrt{2}}{a_3} = \frac{a_3^2}{a_3} = a_3$. Weiter gilt $a_3\varphi_3(a_2) = \varphi_3(a_1)\varphi_3(a_2) = \varphi_3(a_1a_2) = \varphi_3(-2 - \sqrt{2}) = -2 - \varphi_3(\sqrt{2}) \overset{\text{(i)}}{=} -2 + \sqrt{2}$ und daher $\varphi_3(a_2) = \frac{-2+\sqrt{2}}{a_3} = \frac{a_3a_4}{a_3} = a_4$. Schließlich gilt $a_3\varphi_3(a_3) = \varphi_3(a_1)\varphi_3(a_3) = \varphi_3(a_1a_3) = \varphi_3(\sqrt{2}) \overset{\text{(i)}}{=} -\sqrt{2}$ und daher $\varphi_3(a_3) = \frac{-\sqrt{2}}{a_3} = \frac{a_2a_3}{a_3} = a_2$. Da $\varphi_3$ als Automorphismus von $\mathrm{Aut}(L|\mathbb{Q})$ die Nullstellen $a_1, a_2, a_3, a_4$ von $f \in \mathbb{Q}[X]$ permutiert, muss daher $\varphi_3(a_4) = a_1$ sein. Wir haben also $\varphi_3(a_1) = a_3$, $\varphi_3(a_3) = a_2$, $\varphi_3(a_2) = a_4$ und $\varphi_3(a_4) = a_1$. Wenn wir nun wie in der Vorlesung $\mathrm{Aut}(L|\mathbb{Q})$ mit einer Untergruppe der $S_4$ identifizieren, ist $\varphi_3$ ein Viererzykel in $S_4$, nämlich $\varphi_3 = (1\ 3\ 2\ 4)$. Damit gilt in Zykelschreibweise $\varphi_3^2 = (1\ 2)(3\ 4)$ und $\varphi_3^3 = (1\ 4\ 2\ 3)$. Wegen der Eindeutigkeit von $\varphi_i$ aus (g) folgt $\varphi_1 = \varphi_3^0 = 1$, $\varphi_2 = \varphi_3^2 = (1\ 2)(3\ 4)$, $\varphi_3 = (1\ 3\ 2\ 4)$ und $\varphi_4 = \varphi_3^3 = (1\ 4\ 2\ 3)$, was insbesondere auch die Frage beantwortet.

(k) Nach (h) und dem, was wir in (j) gezeigt haben, gilt $\mathrm{Aut}(L|\mathbb{Q}) = \{\varphi_3^0, \varphi_3^1, \varphi_3^2, \varphi_3^3\}$ und $\#\,\mathrm{Aut}(L|\mathbb{Q}) = 4$. Daher ist $\mathrm{Aut}(L|\mathbb{Q})$ zyklisch und somit $\mathrm{Aut}(L|\mathbb{Q}) \cong C_4$.

(l) Nach (f) ist der Hauptsatz der Galoistheorie anwendbar und dieser sagt, dass die Zwischenkörper von $L|\mathbb{Q}$ genau die Fixkörper von Untergruppen von $\mathrm{Aut}(L|\mathbb{Q}) = \{\varphi_3^0, \varphi_3^1, \varphi_3^2, \varphi_3^3\}$ sind. Die beiden trivialen Untergruppen $\{1\}$ und $\mathrm{Aut}(L|\mathbb{Q})$ haben also nach dem Hauptsatz der Galoistheorie natürlich die Fixkörper $L$ und $\mathbb{Q}$. Die einzige nichttriviale Untergruppe ist $H := \{1, \varphi_3^2\} = \{\varphi_1, \varphi_2\}$. Für ihren Fixkörper $F := L^H$ gilt $[L : F] = [H : \{1\}] = \#H = 2$. Da wir in (i) gezeigt haben, dass $\varphi_1(\sqrt{2}) = \varphi_2(\sqrt{2}) = \sqrt{2}$, gilt $\sqrt{2} \in L^H$ und damit $\mathbb{Q}(\sqrt{2}) \subseteq L^H$. Da auch $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ gilt, folgt $L^H = \mathbb{Q}(\sqrt{2})$. Also gibt es genau drei verschiedene Zwischenkörper von $L|\mathbb{Q}$, nämlich $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$ und $L$.

**Bonusaufgabe 7 (12 Bonuspunkte).** Sei $L|K$ eine Körpererweiterung. Betrachte die multiplikativen Gruppen $L^\times$ und $K^\times$ sowie deren Quotientengruppe $L^\times/K^\times$.

(a) Gib eine Bijektion an zwischen $L^\times/K^\times$ und der Menge $\mathscr{U}$ der eindimensionalen Unterräume des $K$-Vektorraums $L$ (mit Beweis). (5 Punkte)

Es sei nun $L^\times/K^\times$ endlich und $L \neq K$.

(b) Zeige, dass $K$ endlich ist. (5 Punkte)

(c) Zeige, dass $L$ endlich ist. (2 Punkte)

**Lösungsvorschlag.** (a) Wir behaupten, dass

$$f\colon L^\times/K^\times \to \mathscr{U},\ xK^\times \to Kx := \{ax \mid a \in K\} \quad (x \in L^\times)$$

eine Bijektion ist. Hierbei ist für $x \in L^\times$ die Menge $xK^\times = \{ax \mid a \in K\}$ die zu $x$ gehörige (Links- oder Rechts-)Nebenklasse von $K^\times$ und $Kx$ der von $x$ aufgespannte eindimensionale $K$-Untervektorraum von $L$. Zur Wohldefiniertheit und Injektivität ist

$$xK^\times = yK^\times \iff Kx = Ky$$

zu zeigen für alle $x, y \in L^\times$ (Wohldefiniertheit ist dabei „ $\Longrightarrow$ “ und Injektivität ist „ $\Longleftarrow$ “). Dies ist praktisch offensichtlich, indem man für „ $\Longrightarrow$ “ die Null auf beiden hinzufügt und sie für „ $\Longleftarrow$ “ auf beiden Seiten entfernt. Schließlich ist die Surjektivität von $f$ klar.

(b) Da $L^\times/K^\times$ nun als endlich vorausgesetzt ist, ist auch $\mathscr{U}$ nach (a) endlich. Für jedes $x \in L$ gibt es aber offensichtlich ein $U \in \mathscr{U}$ mit $x \in U$ (wähle $U = Kx$ für $x \in L^\times$ und $U = K$ für $x = 0$). Also gilt $L = \bigcup \mathscr{U}$. Der $K$-Vektorraum $L$ ist also Vereinigung von $m := \#\mathscr{U}$ vielen Untervektorräumen $\neq L$ (beachte, dass jetzt $L \neq K$ vorausgesetzt ist). Nach einem Lemma aus der Vorlesung ist daher $\#K \leq m - 1$. Insbesondere ist $K$ endlich.

(c) $\#L^\times = [L^\times : K^\times]\#K^\times = (\#(L^\times/K^\times))\#K^\times < \infty$