Universität Konstanz Sabine Burgdorf
Fachbereich Mathematik und Statistik Markus Schweighofer
20. März 2018, Wintersemester 2017/2018

Klausur zur Einführung in die Algebra, Lösungsvorschlag

Aufgabe 1. (a) Seien $x, y, z, x', y', z' \in \mathbb{R}$. Dann

$$\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} x' & y' \\ 0 & z' \end{pmatrix} = \begin{pmatrix} xx' & xy' + yz' \\ 0 & zz' \end{pmatrix}.$$

(b) Seien $x, y, z \in \mathbb{R}$ mit $x \neq 0$ und $z \neq 0$. Dann hat die Matrix $A := \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$ die Determinante $xz \neq 0$ und ist daher invertierbar. Die Komatrix (oder die transponierte klassische Adjungierte) von A ist $\operatorname{com} A = \begin{pmatrix} z & -y \\ 0 & x \end{pmatrix}$, woraus man

$$A^{-1} = \frac{1}{\det A} \operatorname{com} A = \begin{pmatrix} \frac{1}{x} & -\frac{y}{xz} \\ 0 & \frac{1}{z} \end{pmatrix}$$

erhält.

(c) Seien $x, y, z, x', y' \in \mathbb{R}$ mit $x' \neq 0$. Dann

$$\begin{pmatrix} x' & y' \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} x' & y' \\ 0 & 1 \end{pmatrix}^{-1} \underset{\text{(b)}}{\overset{\text{(a)}}{=}} \begin{pmatrix} x'x & x'y + y'z \\ 0 & z \end{pmatrix} \begin{pmatrix} \frac{1}{x'} & -\frac{y'}{x'} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x & x'y + y'z - xy' \\ 0 & z \end{pmatrix}.$$

(d) Jede Matrix aus G ist eine obere Dreiecksmatrix und wegen (b) invertierbar. Dies zeigt „$\subseteq$“. Die andere Inklusion folgt daraus, dass eine invertierbare obere Dreiecksmatrix über einem Körper (oder einem kommutativen Ring) lauter invertierbare Diagonaleinträge hat, denn die Determinante ist invertierbar und sie ist das Produkt der Diagonaleinträge.

(e) Das neutrale Element I_2 von $G = \blacktriangleleft_2(\mathbb{R})$ liegt jeweils in H und in N. Mit der Antwort von (a) sieht man sofort, dass H und N jeweils unter Matrizenmultiplikation abgeschlossen sind. Mit der Antwort von (b) sieht man sofort, dass H und N jeweils unter Matrixinversen abgeschlossen ist. Dies zeigt $H \leq G$ und $N \leq G$. Um nun sogar $N \lhd G$ zu zeigen, fixieren wir ein beliebiges $a \in N$ und $g \in G$ und zeigen $gag^{-1} \in N$. Ohne Einschränkung ist der rechte unter Eintrag von g gleich 1 (sonst multipliziere g mit einem positiven Skalar, was sowohl die Eigenschaft $g \in G$ erhält als auch gag^{-1} nicht ändert). Mit dem Ergebnis aus (c) sieht man, dass die Diagonaleinträge von gag^{-1} gleich den Diagonaleinträgen von a sind, welche positiv sind. Daher $gag^{-1} \in N$.

(f) Wegen (e) ist nur noch zu zeigen, dass $G = NH$ und $N \cap H = \{I_2\}$. Letzteres ist offensichtlich. Um $G = NH$ zu zeigen, seien $x, y, z \in \mathbb{R}$ mit $x \neq 0$ und $z \neq 0$. Dann

$$\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \overset{\text{(a)}}{=} \underbrace{\begin{pmatrix} |x| & y(\operatorname{sgn} z) \\ 0 & |z| \end{pmatrix}}_{\in N} \underbrace{\begin{pmatrix} \operatorname{sgn} x & 0 \\ 0 & \operatorname{sgn} z \end{pmatrix}}_{\in H} \in NH.$$

(g) Seien x, y, z mit $x \neq 0$ und $z \neq 0$. Die Konjugationsklasse von $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$ ist nach dem Ergebnis von (c) und dem Skalierungstrick, der schon in unserer Lösung von (e) angewendet wurde gleich

$$\left\{ \begin{pmatrix} x & x'y + y'z - xy' \\ 0 & z \end{pmatrix} \;\middle|\; x', y' \in \mathbb{R}, x' \neq 0 \right\}.$$

Es gibt eine offensichtliche Bijektion zwischen dieser Konjugationsklasse und der Menge $\{x'y + y'z - xy' \mid x', y' \in \mathbb{R}, x' \neq 0\}$. Ist $y \neq 0$, so ist diese Menge unendlich. Ist $y = 0$, so ist diese Menge offenbar genau dann endlich, wenn $z = x$ und in diesem Fall ist sie einelementig.

(h) Das Zentrum von G besteht offenbar aus den Elementen von G, deren Konjugationsklasse einelementig ist. Wenn ein Normalteiler nicht im Zentrum von G enthalten ist, so enthält er also nach (g) ein Element mit unendlicher Konjugationsklasse. Mit jedem Element enthält aber ein Normalteiler auch dessen ganze Konjugationsklasse.

(i) Wie gesagt besteht das Zentrum von G besteht aus den Elementen von G, deren Konjugationsklasse einelementig ist. Im Beweis von (g) haben wir schon gesehen, dass somit $Z(G)$ aus allen Matrizen der Form $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$ mit $y = 0$ und $x = z$ besteht.

(j) Wegen (i) ist $\mathbb{R}^\times \to Z(G),\ \lambda \mapsto \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ offenbar ein Gruppenisomorphismus.

(k) Offensichtlich enthält $\mathbb{R}^\times$ nur zwei endliche Untergruppen, nämlich $\{1\}$ und $\{-1, 1\}$. Alle anderen Untergruppen von $\mathbb{R}^\times$ sind nämlich offensichtlich unbeschränkte Teilmengen von $\mathbb{R}$. Insbesondere hat $\mathbb{R}^\times$ und damit auch die nach (j) dazu isomorphe Gruppe $Z(G)$ keine vierelementige Untergruppe.

(l) Da $H \cong C_2 \times C_2$ offensichtlich abelsch ist, gilt $\{1\} \times H \leq Z(N \times H)$.

(m) folgt direkt aus (k) und (l).

Aufgabe 2. (a) Bezeichne $\varphi\colon \mathbb{Z} \to \mathbb{Z}/(20)$ den kanonischen Epimorphismus. Die Zuordnungen

$$\begin{aligned} I &\mapsto \varphi(I) \\ \varphi^{-1}(I) &\mapsfrom J \end{aligned}$$

vermitteln dann eine inklusionsumkehrende Bijektion zwischen den Idealen von $\mathbb{Z}$, die die Zahl 20 enthalten, und den Idealen von $\mathbb{Z}/(20)$. Da $\mathbb{Z}$ ein Hauptidealring ist, werden die Ideale in $\mathbb{Z}$, die die Zahl 20 enthalten, genau durch die positiven Teiler von 20 in $\mathbb{Z}$ erzeugt. Die sechs verschiedenen Ideale (1), (2), (4), (5), (10) und (20) sind somit genau die Ideale von $\mathbb{Z}$, die 20 enthalten. Unter der obigen Bijektion werden sie abgebildet auf die Ideale

$$\begin{aligned}
J_1 &:= \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}, \overline{15}, \overline{16}, \overline{17}, \overline{18}, \overline{19}\},\\
J_2 &:= \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}, \overline{18}\},\\
J_4 &:= \{\overline{0}, \overline{4}, \overline{8}, \overline{12}, \overline{16}\},\\
J_5 &:= \{\overline{0}, \overline{5}, \overline{10}, \overline{15}\},\\
J_{10} &:= \{\overline{0}, \overline{10}\} \qquad \text{und}\\
J_{20} &:= \{\overline{0}\},
\end{aligned}$$

wobei natürlich jeweils $\overline{a}$ die Restklasse von $a \in \mathbb{Z}$ modulo (20) bezeichne.

(b) Aus der Vorlesung weiß man, dass die in (a) genannten Zuordnungen ebenfalls eine inklusionsumkehrende Bijektion zwischen den *Prim*idealen von $\mathbb{Z}$, die die Zahl 20 enthalten, und den *Prim*idealen von $\mathbb{Z}/(20)$ vermitteln. Da $\mathbb{Z}$ ein Hauptidealring ist, werden die Ideale in $\mathbb{Z}$, die die Zahl 20 enthalten, genau durch die positiven *Prim*teiler von 20 in $\mathbb{Z}$ erzeugt, also von 2 und 5. Somit sind J_2 und J_5 genau die beiden verschiedenen Primideale von $\mathbb{Z}/(20)$. Da keines der beiden im jeweils anderen enthalten ist, sind sie beide auch maximal.

Aufgabe 3. (a) Wegen $p = 0$ in $\mathbb{F}_p$ handelt es sich hier um das Polynom $X^3 \in \mathbb{F}_p[X]$, welches wegen $X^3 = XX^2$ und $X, X^2 \notin \mathbb{F}_p^\times = \mathbb{F}_[X]^\times$ nicht irreduzibel ist.

(b) Wegen $p = 0$ in $\mathbb{F}_{p^2}$ ist genauso wie in (a) das Polynom nicht irreduzibel in $\mathbb{F}_{p^2}[X]$.

(c) Wir behaupten, dass das gegebene Polynom irreduzibel in $\mathbb{Z}[X]$ ist. Zunächst liegt das Polynom sicher nicht in $\mathbb{Z}[X]^\times = \mathbb{Z}^\times$. Angenommen das Polynom ist irreduzibel. Dann gibt es $f, g \in \mathbb{Z}[X] \setminus \mathbb{Z}$ mit $X^3 + pX^2 + p^2 = fg$. Es muss dann $\deg f + \deg g = 3$ gelten. Nach etwaigem Vertauschen von f und g können wir von $\deg f = 1$ und $\deg g = 2$ ausgehen. Das Produkt der Leitkoeffizienten von f und g muss 1 sein, also müssen sie Einheiten sein. Nach eventueller gleichzeitiger Vorzeichenänderung von f und g können wir daher davon ausgehen, dass f und g normiert sind. Schreibe $f = X + a$ mit $a, b \in \mathbb{Z}$. Dann ist a ein Teiler von p^2 in $\mathbb{Z}$. Da $\mathbb{Z}$ faktoriell und p prim ist, folgt daraus $a \in \{-p^2, -p, -1, 1, p, p^2\}$. Ausserdem ist aber a eine Nullstelle von f und daher von $X^3 + pX^2 + p^2$. Daher kann a nicht positiv sein. Also $a \in \{-p^2, -p, -1\}$. Wäre $a = -1$, so $-1 + p + p^2 = 0$ ↯. Wäre $a = -p$, so $-p^3 + p^3 + p^2 = 0$ ↯. Wäre $a = -p^2$, so $-p^6 + p^5 + p^2 = 0$ und daher $p^3 + 1 = p^4$, was $1 = 0$ in $\mathbb{Z}/(p)$ implizierte ↯. Insgesamt erhalten wir also in jedem Fall einen Widerspruch zu unserer Annahme, dass das Polynom irreduzibel in $\mathbb{Z}[X]$ ist.

(d) Da $\mathbb{Z}$ ein faktorieller Ring mit Quotientenkörper $\mathbb{Q}$ ist und das gegebene Polynom vom Grad ≥ 1 ist, impliziert die in (c) bewiesene Irreduzibilität des Polynoms in $\mathbb{Z}[X]$ auch seine Irreduzibilität in $\mathbb{Q}[X]$.

(e) Da es ungeraden Grad hat, hat das Polynom nach dem Zwischenwertsatz aus der Analysis eine Nullstelle. Wenn man den dazugehörigen Linearfaktor abspaltet, bekommt man eine nichttriviale Zerlegung, die zeigt, dass das Polynom in $\mathbb{R}[X]$ reduzibel ist.

(f) Wie in (e) (oder alternativ einfach mit dem Fundamentalsatz der Algebra) folgt genauso wie in (e), dass das Polynom in $\mathbb{C}[X]$ reduzibel ist.

Aufgabe 4. Falls $p = q$, so ist G eine p-Gruppe und nach Vorlesung daher auflösbar. Dann folgt die Behauptung sofort aus dem Satz über die Existenz von Normalreihen mit Faktoren von Primzahlordnung. Sei also nun $p \neq q$. Aus Symmetriegründen können wir Œ von $q < p$ ausgehen. Für die Anzahl n_p der p-Sylowgruppen von G gilt $p \mid (n_p - 1)$ und $n_p \mid pq$. Wegen $p \mid (n_p - 1)$ kann p kein Teiler von n_p sein (sonst wäre p ein Teiler von 1). Also $n_p \in \{1, q\}$. Aus $p > q$ und $p \mid (n_p - 1)$ folgt dann $n_p = 1$. Es besitzt G also genau eine p-Sylowgruppe N von G. Da jeder Isomorphismus und damit insbesondere jeder innere Automorphismus von G daher natürlich N auf N abbilden muss, ist N ein Normalteiler von G und tut das Gewünschte.

Aufgabe 5. Seien $x, y \in \overline{K}$ beliebig mit $x^2 = a$ und $y^2 = b$ (für später sei auch bemerkt, dass es natürlich solche x und y gibt, da die Polynome $X^2 - a$ und $X^2 - b$ jeweils eine Nullstelle in $\overline{K}$ haben). Dann rechnet man sofort $X^2 - a = (X - x)(X + x)$ und $X^2 - b = (X - y)(X + y)$ nach. Folglich $(X^2 - a)(X^2 - b) = (X - x)(X + x)(X - y)(X + y)$.

(a) Es ist f separabel genau dann die Menge $\{-x, x, -y, y\}$ vierelementig ist. Wegen $\operatorname{char} K \neq 2$ sind die beiden Mengen $\{-x, x\}$ und $\{-y, y\}$ jeweils zweielementig. Daher ist f separabel genau dann, wenn $\{-x, x\} \cap \{-y, y\} = \emptyset$. Dies ist der Fall, wenn $a \neq b$, denn dann $(\pm x)^2 = a \neq b = (\pm y)^2$. Ist dies umgekehrt der Fall, so haben $X^2 - a$ und $X^2 - b$ keine gemeinsame Nullstelle in $\overline{K}$ und müssen daher verschiedene Polynome sein, das heißt $a \neq b$. Damit ist (a) gezeigt, wobei wir die obige Bemerkung über die Existenz von x und y benutzt haben.

(b) Gelte nun $a \neq b$.
Lösung von Sabine Burgdorf:

$$L = K(x, -x, y, -y) = K(x, y) \overset{\operatorname{char} K \neq 2}{=} K(x - y, x + y) \overset{\substack{\text{Trick:} \\ x - y = \frac{a-b}{x+y}}}{=} K(x + y).$$

Lösung von Markus Schweighofer: Wegen $a \neq b$ ist nach (a) der Körper L der Zerfällungskörper des separablen Polynoms f über K, dessen Nullstellen $a_1 := x$, $a_2 := -x$, $a_3 := y$ und $a_4 := -y$ sind und damit $L|K$ eine endliche Galoiserweiterung, deren Galoisgruppe G wir dementsprechend als Untergruppe von S_4 auffassen. Wegen $X^2 - a, X^2 - b \in K[X]$ gilt dann offensichtlich $G \leq \{1, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$. Um

$L = K(x+y)$ zu zeigen, reicht es nach Galoistheorie zu zeigen, dass die Galoisgruppen von $L|L$ und $L|K(x+y)$ gleich sind, das heißt, dass der einzige Automorphismus von $L|K$, der $x+y$ fest lässt, die Identität ist. Hierzu reicht es zu zeigen, dass die bis zu drei nichtneutralen Elemente von G jeweils $x+y$ nicht fest lassen. Potentielle Bilder von $x+y$ unter einem nichtneutralen Element von G sind aber nur $-x+y$, $x-y$ und $-(x+y)$. Wegen $\operatorname{char} K \neq 2$ gilt aber $x+y \neq -x+y$, $x+y \neq x-y$ und $x+y \neq -(x+y)$ (für letzteres benutze $x \neq y$, was sofort aus $a \neq b$ folgt).

Aufgabe 6. (a) Da die multiplikative Gruppe von $\mathbb{F}_p$ die Ordnung $p-1$ hat, gilt $x^{p-1} = 1$ für alle $x \in \mathbb{F}_p^\times$ und daher $x^p = x$ für alle $x \in \mathbb{F}_p$. Andererseits gilt

$$b^p = f(b) + b - a \overset{f(b)=0}{=} b - a \overset{a\neq 0}{\neq} b.$$

(b)

$$\begin{aligned} f(X+1) &= (X+1)^p - (X+1) + a = \Phi_{\mathbb{F}_p[X]}(X+1) - X - 1 + a \\ &= \Phi_{\mathbb{F}_p[X]}(X) + 1 - X - 1 + a = f \end{aligned}$$

(c) Da f normiert vom Grad p ist, reicht es zu zeigen, dass $f(b+c) = 0$ für alle $c \in \mathbb{F}_p$. Dazu reicht es durch Induktion nach n zu zeigen, dass $f(b + \overline{n}^{(p)}) = 0$ für alle $n \in \mathbb{N}_0$. Für $n = 0$ folgt dies aus $f(b) = 0$. Ist ferner $n \in \mathbb{N}$ mit $f(b + \overline{n-1}^{(p)}) = 0$, so folgt $f(b + \overline{n}^{(p)}) = f(b + \overline{n-1}^{(p)} + 1) \overset{\text{(b)}}{=} f(b + \overline{n-1}^{(p)}) = 0$.

(d) Setze $g := \operatorname{irr}_{\mathbb{F}_p}(b)$. Da $\mathbb{F}_p$ als endlicher Körper vollkommen ist, ist g separabel. Wegen (a) gilt $\deg g \geq 2$. Daher gibt es $x, y \in \overline{\mathbb{F}}_p$ mit $x \neq y$ und $g(x) = g(y) = 0$. Wegen $f(b) = 0$ gilt $f \in (g)_{\mathbb{F}_p[X]}$ und daher auch $f(x) = f(y) = 0$. Wegen (c) können wir $c, d \in \mathbb{F}_p$ wählen mit $x = b + c$ und $y = b + d$. Wegen $c \neq d$, können wir dabei Œ von $c \neq 0$ ausgehen, also $c \in \mathbb{F}_p^\times$.

(e) Betrachte c und d wie in unserem Beweis von (d) gewählt. Wir zeigen, dass es ein $\sigma \in \operatorname{Aut}(\overline{\mathbb{F}}_p|\mathbb{F}_p)$ gibt mit $\sigma(b) = b + (d-c)$, was gleichbedeutend mit $\sigma(b+c) = b+d$ ist. Dies ist aber nach Vorlesung klar, da $b+c$ und $b+d$ dasselbe Minimalpolynom über $\mathbb{F}_p$ haben und daher über $\mathbb{F}_p$ konjugiert sind.

(f) Betrachte $G := \{c \in \mathbb{F}_p \mid \exists \sigma \in \operatorname{Aut}(\overline{\mathbb{F}}_p|\mathbb{F}_p) : \sigma(b) = b + c\}$. Da $\operatorname{Aut}(\overline{\mathbb{F}}_p|\mathbb{F}_p)$ eine Untergruppe aller Permutationen von $\overline{\mathbb{F}}_p$ ist, sieht man leicht, dass G eine Untergruppe der additiven Gruppe von $\mathbb{F}_p$ ist. Da die Gruppenordnung von G ein Teiler der Primzahl p ist, reicht es zu zeigen, dass G ein Element aus $\mathbb{F}_p \setminus \{0\}$ enthält, was ja gerade in (e) bewiesen wurde.

(g) Offenbar gilt $f \notin \mathbb{F}_p[X]^\times = \mathbb{F}_p^\times$, denn $\deg f = p$. Nach (c) und (f) wirkt $\operatorname{Aut}(\overline{\mathbb{F}}_p|\mathbb{F}_p)$ transitiv auf den Nullstellen von f in $\overline{\mathbb{F}}_p$. Gäbe es $g, h \in \mathbb{F}_[X] \setminus \mathbb{F}_p$ mit $f = gh$, so Œ $g(b) = 0$ und die Bahn von b unter dieser Wirkung hätte höchstens $\deg p < p$ viele Elemente.

(h) Es ist $\mathbb{F}_p(b) = \mathbb{F}_p(\{b + c \mid c \in \mathbb{F}_p\})$ gemäß (c) der Zerfällungskörper des nach (c) separablen Polynoms f.

(i) Wegen (g) gilt $f = \operatorname{irr}_{\mathbb{F}_p}(b)$ und daher $[\mathbb{F}_p(b) : \mathbb{F}_p] = \deg f = p$. Daher ist $\mathbb{F}_p(b)$ ein zweidimensionaler $\mathbb{F}_p$-Vektorraum und damit als $\mathbb{F}_p$-Vektorraum isomorph zu $\mathbb{F}_p^2$. Insbesondere hat $\mathbb{F}_p(b)$ genau p^2 viele Elemente. Damit gilt schon mal $\mathbb{F}_p(b) \cong \mathbb{F}_{p^2}$. Da aber $\mathbb{F}_p(b)$ ein Zwischenkörper von $\overline{\mathbb{F}}_p|\mathbb{F}_p$ ist, gilt sogar $\mathbb{F}_p(b) = \mathbb{F}_{p^2}$.

Aufgabe 8. (a) Wegen

$$f = (X^2 + 2)(X^2 + 3) = (X - \mathring{\imath}\sqrt{2})(X + \mathring{\imath}\sqrt{2})(X - \mathring{\imath}\sqrt{3})(X + \mathring{\imath}\sqrt{3})$$

sind

$$a_1 := -\mathring{\imath}\sqrt{2},\ a_2 := \mathring{\imath}\sqrt{2},\ a_3 := -\mathring{\imath}\sqrt{3} \text{ und } a_4 := \mathring{\imath}\sqrt{3}$$

genau die vier verschiedenen Nullstellen von f in $\mathbb{C}$. Nach einer Bemerkung aus der Vorlesung ist daher $L|\mathbb{Q}$ eine Galoiserweiterung und wir können die Galoisgruppe G von $L|\mathbb{Q}$ im Folgenden als Untergruppe der S_4 auffassen.

(b) Wegen $(X - a_1)(X - a_2) \in \mathbb{Q}[X]$ und $(X - a_3)(X - a_4) \in \mathbb{Q}[X]$, gilt

$$G \subseteq \{1, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}.$$

Nach Galoistheorie gilt ferner $\#G = [L : \mathbb{Q}]$. Wir zeigen, dass $[L : \mathbb{Q}] = 4$, woraus dann

$$G = \{1, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$$

folgt, das heißt G ist isomorph zur Kleinschen Vierergruppe (nummeriere die Seiten eines Rechtecks geeignet). Wegen $L = \mathbb{Q}(a_1, a_2, a_3, a_4) = \mathbb{Q}(\mathring{\imath}\sqrt{2}, \mathring{\imath}\sqrt{3})$ erhält man aus $[\mathbb{Q}(\mathring{\imath}\sqrt{3}) : \mathbb{Q}] = 2$ und aus der Gradformel

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\mathring{\imath}\sqrt{2})][\mathbb{Q}(\mathring{\imath}\sqrt{2}) : \mathbb{Q}] = [L : \mathbb{Q}(\mathring{\imath}\sqrt{2})]2.$$

Es reicht daher $\mathring{\imath}\sqrt{3} \notin \mathbb{Q}(\mathring{\imath}\sqrt{2})$ zu zeigen. Angenommen wir hätten $\mathring{\imath}\sqrt{3} \in \mathbb{Q}(\mathring{\imath}\sqrt{2})$. Wir suchen einen Widerspruch. Wegen $[\mathbb{Q}(\mathring{\imath}\sqrt{2}) : \mathbb{Q}] = 2$, gibt es $a, b \in \mathbb{Q}$ mit $\mathring{\imath}\sqrt{3} = a + b\mathring{\imath}\sqrt{2}$. Quadriert man dies, so erhält man $-3 = a^2 - 2ab\sqrt{2} - 2b^2$ und daher $ab = 0$. Ist $b = 0$, so $a^2 + 3 = 0$, was aus Positivitätsgründen unmöglich. Ist $a = 0$, so $-3 = -2b^2$, was aus Paritätsgründen unmöglich ist. In beiden Fällen haben wir also einen Widerspruch.

(c) Die Untergruppen von G sind offensichtlich

$$\{1\}, \quad \{1, (1\ 2)\} \quad \{1, (3\ 4)\} \quad \text{und} \quad \{1, (1\ 2)(3\ 4)\}.$$

Die jeweils dazugehörigen Fixkörper sind in derselben Reihenfolge

$$L, \quad \mathbb{Q}(\mathring{\imath}\sqrt{3}), \quad \mathbb{Q}(\mathring{\imath}\sqrt{2}) \quad \text{und} \quad \mathbb{Q}(\mathring{\imath}\sqrt{2}\,\mathring{\imath}\sqrt{3}) = \mathbb{Q}(\sqrt{6}),$$

denn diese Körper sind jeweils offensichtlich im Fixkörper enthalten und haben den Grad des Fixkörpers über $\mathbb{Q}$ (nämlich die Ordnung der jeweiligen Untergruppe). Nach dem Hauptsatz der Galoistheorie sind diese vier Körper genau die Zwischenkörper von $L|\mathbb{Q}$.