Lösungen zur Algebra-Klausur vom 1.4.2008

Aufgabe 1
Es sei G eine endliche Gruppe mit $G \neq \{1\}$. Je zwei Elemente aus $G \setminus \{1\}$ seien konjugiert. Wie viele Elemente hat G?

Lösung:
Es ist klar, dass für die Gruppe $\mathbb{Z}/2\mathbb{Z}$ die geforderten Eigenschaften gelten. Wir zeigen nun, dass jede Gruppe G, die die geforderten Eigenschaften erfüllt, zwei Elemente hat.

1. Lösung:

- Je zwei Elemente $x, y \in G \setminus \{1\}$ haben dieselbe Ordnung:
  x, y konjugiert $\Rightarrow \exists\, g \in G:\ x = gyg^{-1}$
  $\Rightarrow x^{\mathrm{ord}(y)} = gy^{\mathrm{ord}(y)}g^{-1} = g1g^{-1} = 1$ und $y^{\mathrm{ord}(x)} = g^{-1}x^{\mathrm{ord}(x)}g = g^{-1}1g = 1$
  $\Rightarrow \mathrm{ord}(x) \leq \mathrm{ord}(y)$ und $\mathrm{ord}(y) \leq \mathrm{ord}(x)$
  $\Rightarrow \mathrm{ord}(x) = \mathrm{ord}(y)$

- G ist eine p-Gruppe für eine Primzahl p:
  Annahme: $|G|$ hat verschiedene Primteiler p, q.
  $\Rightarrow |G| = p^r q^s m$ für geeignete $r, s \geq 1$, $m \geq 1$, p, q keine Teiler von m.
  $\overset{\text{Sylow}}{\Rightarrow}$ Es gibt $x, y \in G$ mit $\mathrm{ord}(x) = p$, $\mathrm{ord}(y) = q$.
  Das ist ein Widerspruch zu $\mathrm{ord}(x) = \mathrm{ord}(y)$.

- Als p-Gruppe hat G ein nichttriviales Zentrum.
  Seien $x \in Z(G) \setminus \{1\}$ und $y \in G \setminus \{1\}$.
  $\Rightarrow \exists\, g \in G:\ x = gyg^{-1}$
  $\Rightarrow y = g^{-1}xg \overset{x \in Z(G)}{=} xg^{-1}g = x$
  $\Rightarrow G = \{1, x\} \cong \mathbb{Z}/2\mathbb{Z}$ und $|G| = 2$

2. Lösung:
G operiert auf sich selbst durch Konjugation. Nach Voraussetzung gibt es genau zwei Bahnen $\{1\}$ und $G \setminus \{1\}$. Die Ordnung jeder Bahn ist ein Teiler der Gruppenordnung ($\rightarrow$ Bahnbilanz), d.h. $|G| - 1$ ist ein Teiler von $|G|$.
$\Rightarrow |G| = 2$

Aufgabe 2

a) Was sagt der Struktursatz für endlich erzeugte abelsche Gruppen?

b) Zeigen Sie:

Ist G eine endlich erzeugte abelsche Gruppe und $H \leq G$ eine Untergruppe von G, so ist H endlich erzeugt.

c) Gilt die Aussage aus b) auch für nichtabelsche, endlich erzeugte Gruppen?

Lösung:

a) Ist G eine endlich erzeugte abelsche Gruppe, so gibt es eindeutige $r, m \in \mathbb{N}$ und $a_1, \ldots, a_m \in \mathbb{N}_{\geq 2}$ mit $a_1 \mid a_2 \mid \ldots \mid a_m$ und $G \cong \mathbb{Z}^r \times \prod_{i=1}^{m} \mathbb{Z}/a_i\mathbb{Z}$.

b) **1. Lösung:**
Nach dem Struktursatz gibt es $r, m \in \mathbb{N}$ und $a_1, \ldots, a_m \in \mathbb{N}_{\geq 2}$ mit $G \cong \mathbb{Z}^r \times \prod_{i=1}^{m} \mathbb{Z}/a_i\mathbb{Z}$. Sei o.E. $G = \mathbb{Z}^r \times \prod_{i=1}^{m} \mathbb{Z}/a_i\mathbb{Z}$.
Seien $\hat{G} := \mathbb{Z}^{r+m}$ und $\Phi : \hat{G} \to G$, $(x_1, \ldots, x_r, y_1, \ldots, y_m) \mapsto (x_1, \ldots, x_r, y_1 + a_1\mathbb{Z}, \ldots, y_m + a_m\mathbb{Z})$ die kanonische Projektion. Φ ist surjektiv. Sei $\hat{H} := \Phi^{-1}(H) \leq \hat{G}$. Nach dem Elementarteilersatz ist $\hat{H}$ endlich erzeugt, denn $\hat{H}$ ist eine freie abelsche Gruppe vom Rang $\leq r + m$. Seien $\hat{h}_1, \ldots, \hat{h}_s \in \hat{H}$ mit $\hat{H} = \langle \hat{h}_1, \ldots, \hat{h}_s \rangle$.
$\Rightarrow H = \Phi(\hat{H}) = \Phi(\langle \hat{h}_1, \ldots, \hat{h}_s \rangle) = \langle \Phi(\hat{h}_1), \ldots, \Phi(\hat{h}_s) \rangle$
$\Rightarrow H$ ist endlich erzeugt.

2. Lösung:
Nach dem Struktursatz gibt es ein $r \in \mathbb{N}$ und eine endliche abelsche Gruppe T mit $G \cong \mathbb{Z}^r \times T$. Sei o.E. $G = \mathbb{Z}^r \times T$. Für $H \leq G$ definieren wir:
$H_1 := \{a \in \mathbb{Z}^m : (a, 0) \in H\} \leq \mathbb{Z}^r$,
$H_2 := \{t \in T : \text{es gibt ein } s \in \mathbb{Z}^r \text{ mit } (s, t) \in H\} \leq T$.
Als Untergruppe von $\mathbb{Z}^r$ ist H_1 nach dem Elementarteilersatz endlich erzeugt, schreibe $H_1 = \langle a_1, \ldots, a_k \rangle$ mit geeigneten $a_1, \ldots, a_k \in \mathbb{Z}^r$. Als Untergruppe der endlichen Gruppe T ist H_2 endlich, schreibe $H_2 = \{t_1, \ldots, t_l\}$. Nach Definition von H_2 gibt es $s_1, \ldots, s_l \in \mathbb{Z}^r$ mit $h_i := (s_i, t_i) \in H$ $(i = 1, \ldots, l)$.
Beh.: $H = \langle (a_1, 0), \ldots, (a_k, 0), h_1, \ldots, h_l \rangle$ und somit ist H endlich erzeugt.

"$\supseteq$": Nach Definition von H_1 sind alle $(a_i, 0) \in H$ $(i = 1, \ldots k)$.
Nach Definition der h_i sind alle $h_i \in H$ $(i = 1, \ldots l)$.

"$\subseteq$": Sei $h = (x, y) \in H$ mit $x \in \mathbb{Z}^r$ und $y \in T$.
$\Rightarrow y \in H_2 \Rightarrow y = t_i$ für ein $i \in \{1, \ldots, l\}$
$\Rightarrow h - h_i = (x, y) - (s_i, t_i) = (x - s_i, 0) \in H$
$\Rightarrow x - s_i \in H_1$, d.h. $x - s_i$ ist ein Wort in $a_1, \ldots, a_k$.
$\Rightarrow h - h_i = (x - s_i, 0)$ ist ein Wort in $(a_1, 0), \ldots, (a_k, 0)$.
$\Rightarrow h - h_i \in \langle (a_1, 0), \ldots, (a_k, 0) \rangle$
$\Rightarrow h \in \langle (a_1, 0), \ldots, (a_k, 0), h_i \rangle \subseteq \langle (a_1, 0), \ldots, (a_k, 0), h_1, \ldots, h_l \rangle$

Für die Erfahreneren unter uns können wir die zweite Lösung auch kürzer formulieren: Wir haben die exakte Sequenz $1 \to \mathbb{Z}^r \xrightarrow{\iota} \mathbb{Z}^r \times T \xrightarrow{p} T \to 1$. Für eine Untergruppe $H \leq \mathbb{Z}^r \times T$ ist also auch die Sequenz

$$1 \to \iota^{-1}(H) \to H \to p(H) \to 1$$

exakt. Da $\iota^{-1}(H)$ (nach dem Elementarteilersatz) und $p(H)$ (als endliche Menge) endlich erzeugt sind, ist es auch H.

c) Sei $G = F_2 = F(x,y)$ die freie Gruppe vom Rang 2 mit Basis $\{x,y\}$. Wegen $G = \langle x,y\rangle$ ist G endlich erzeugt. Sei $H := \langle\{y^i x y^{-i} : i \in \mathbb{Z}\}\rangle$.

Annahme: H ist endlich erzeugt, zum Beispiel von den Elementen $a_1, \ldots, a_n \in H$. Dann wird H auch von endlich vielen der vorgegebenen Erzeuger $y^i x y^{-i}$ erzeugt, denn jedes der endlich vielen a_j kann als endliches Wort in diesen Erzeugern dargestellt werden.
$\Rightarrow$ Es gibt ein $m \in \mathbb{N}$ mit $H = \underbrace{\langle\{y^i x y^{-i} : |i| \leq m\}\rangle}_{=:H'}$.
Wir führen das zu einem Widerspruch, indem wir zeigen, dass $y^{m+1}xy^{-(m+1)}$ nicht in H' enthalten ist. Dazu beweisen wir folgende Hilfsaussage:

- Beh.: Jedes Wort $w \in H' \setminus \{1\}$ endet mit den Buchstaben $x^\varepsilon y^{-i}$ für ein $\varepsilon = \pm 1$ und ein i mit $|i| \leq m$.
  denn:
  Jedes $w \in H'$ kann geschrieben werden als $w = (y^{i_1}xy^{-i_1})^{\varepsilon_1} \cdot \ldots \cdot (y^{i_k}xy^{-i_k})^{\varepsilon_k}$ mit $k \in \mathbb{N}$, $i_1, \ldots, i_k \in \{-m, \ldots, m\}$, $\varepsilon_1, \ldots, \varepsilon_k \in \{1, -1\}$ und $(y^{i_\nu}xy^{-i_\nu})^{\varepsilon_\nu} \neq (y^{i_{\nu+1}}xy^{-i_{\nu+1}})^{-\varepsilon_{\nu+1}}$ $(\nu = 1, \ldots, k-1)$. Wir zeigen die Aussage induktiv:

  $k = 0 \Rightarrow w = 1$ und es ist nichts zu zeigen.
  $k = 1 \Rightarrow w = (y^{i_1}xy^{-i_1})^{\varepsilon_1} = y^{i_1}x^{\varepsilon_1}y^{-i_1}$
  $k \to k+1$:
  Es ist $w = \tilde{w} \cdot (y^{i_{k+1}}xy^{-i_{k+1}})^{\varepsilon_{k+1}}$ für ein geeignetes $\tilde{w} \in H'$, das nach Induktionsvoraussetzung (als reduziertes Wort) geschrieben werden kann als $\tilde{w} = vx^\varepsilon y^{-i}$. Damit ist $w = vx^\varepsilon y^{-i+i_{k+1}}x^{\varepsilon_{k+1}}y^{-i_{k+1}}$. Für $i \neq i_{k+1}$ ist das reduziert und von der gewünschten Form. Ist jedoch $i = i_{k+1}$, so gilt zusätzlich $\varepsilon = \varepsilon_{k+1}$, und auch in diesem Fall ist $w = vx^\varepsilon x^\varepsilon y^{-i_{k+1}}$ von der gewünschten Form.

Wäre nun $y^{m+1}xy^{-(m+1)} \in H'$, so würde es mit den Buchstaben $x^{\pm 1}y^{-i}$ für ein i mit $|i| < m+1$ enden, was es aber offensichtlich nicht tut.

Insgesamt erhalten wir:
G ist eine endlich erzeugte Gruppe und $H \leq G$ ist eine Untergruppe, die nicht endlich erzeugt ist.

Aufgabe 3
Es sei R ein kommutativer Ring mit Eins. Beweisen oder widerlegen Sie die folgenden Aussagen:

a) Ist R nullteilerfrei, so ist für jedes Primideal $P \lhd R$ die Lokalisierung R_P nullteilerfrei.

b) Ist für jedes Primideal $P \lhd R$ die Lokalisierung R_P nullteilerfrei, so ist R nullteilerfrei.

Lösung:

a) Sei R nullteilerfrei. Sei $P \lhd R$ ein Primideal.
$\Rightarrow R_P = \{\frac{r}{s} : r \in R, s \in R \setminus P\} \subseteq \text{Quot}(R)$
Seien $x_1 = \frac{r_1}{s_1}$, $x_2 = \frac{r_2}{s_2} \in R_P$ mit $x_1 \cdot x_2 = 0$.
$\Rightarrow \frac{0}{1} = \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$
$\Rightarrow r_1 r_2 \cdot 1 - s_1 s_2 \cdot 0 = 0$ (da R nullteilerfrei)
$\Rightarrow r_1 r_2 = 0 \Rightarrow r_1 = 0$ oder $r_2 = 0$ (da R nullteilerfrei)
$\Rightarrow x_1 = \frac{r_1}{s_1} = 0$ oder $x_2 = \frac{r_2}{s_2} = 0$
$\Rightarrow R_P$ ist nullteilerfrei.

b) **1. Lösung:**
Seien K, L Körper. $K \times L$ ist mit komponentenweiser Verknüpfung ein kommutativer Ring mit Eins. $K \times L$ ist nicht nullteilerfrei, da zum Beispiel $(1,0)\cdot(0,1) = (0,0)$. Die Ideale von $K \times L$ sind $\{(0,0)\}$, $K \times \{0\}$, $\{0\} \times L$ und $K \times L$. Davon sind $K \times \{0\}$ und $\{0\} \times L$ Primideale, sogar maximale Ideale. ($\{(0,0)\}$ und $K \times L$ sind offensichtlich keine Primideale.)

Es ist $(K \times L)_{K\times\{0\}} = \{\frac{(a,b)}{(x,y)} : a, x \in K, b, y \in L, y \neq 0\}$. Die Darstellung $\frac{(a,b)}{(x,y)}$ für ein Element aus $(K \times L)_{K\times\{0\}}$ ist dabei nicht eindeutig.

Behauptung: $\Phi : L \to (K \times L)_{K\times\{0\}}$, $b \mapsto \frac{(0,b)}{(0,1)}$ ist ein Isomorphismus.

- $\Phi(b_1 + b_2) = \frac{(0,b_1+b_2)}{(0,1)} = \frac{(0,b_1)+(0,b_2)}{(0,1)} = \frac{(0,b_1)}{(0,1)} + \frac{(0,b_2)}{(0,1)} = \Phi(b_1) + \Phi(b_2)$
  $\Phi(b_1 b_2) = \frac{(0,b_1 b_2)}{(0,1)} = \frac{(0,b_1)\cdot(0,b_2)}{(0,1)\cdot(0,1)} = \frac{(0,b_1)}{(0,1)} \cdot \frac{(0,b_2)}{(0,1)} = \Phi(b_1) \cdot \Phi(b_2)$
  $\Phi(1) = \frac{(0,1)}{(0,1)} \overset{\text{erweitern}}{=} \frac{(0,1)\cdot(1,1)}{(0,1)\cdot(1,1)} \overset{\text{kürzen}}{=} \frac{(1,1)}{(1,1)} = 1$
  $\Rightarrow \Phi$ ist ein Homomorphismus von Ringen mit Eins.
- Sei $b \in L$ mit $\Phi(b) = 0$.
  $\Rightarrow \frac{(0,b)}{(0,1)} = \frac{(0,0)}{(1,1)}$
  $\Rightarrow \exists\, s \in K,\ t \in L \setminus \{0\} :\ (s,t) \cdot [(0,b) \cdot (1,1) - (0,1) \cdot (0,0)] = (0,0)$
  $\Rightarrow \exists\, s \in K,\ t \in L \setminus \{0\} :\ (s,t) \cdot (0,b) = (0,0)$
  $\Rightarrow \exists\, t \in L \setminus \{0\} :\ tb = 0$
  $\Rightarrow b = 0$
  $\Rightarrow \Phi$ ist injektiv.
- Sei $\frac{(a,b)}{(x,y)} \in (K \times L)_{K\times\{0\}}$ mit $a, x \in K$, $b, y \in L$, $y \neq 0$.
  $\Rightarrow \frac{(a,b)}{(x,y)} \overset{\text{erweitern}}{=} \frac{(a,b)\cdot(0,y^{-1})}{(x,y)\cdot(0,y^{-1})} = \frac{(0,y^{-1}b)}{(0,1)} = \Phi(y^{-1}b) \in \text{Bild}(\Phi)$
  $\Rightarrow \Phi$ ist surjektiv.

Insgesamt ist $(K \times L)_{K\times\{0\}} \cong L$ ein Körper und somit nullteilerfrei.
genauso: $(K \times L)_{\{0\}\times L} \cong K$ ist nullteilerfrei.

2. Lösung:
Sei $R := \mathbb{Z}/6\mathbb{Z} = \{\tilde{0}, \tilde{1}, \ldots, \tilde{5}\}$. R ist nicht nullteilerfrei. R hat die Ideale $\{\tilde{0}\}$, $I := \{\tilde{0}, \tilde{2}, \tilde{4}\}$, $J = \{\tilde{0}, \tilde{3}\}$ und R. Davon sind I und J Primideale, sogar maximale Ideale.

Es ist $R_I = \{\frac{\tilde{a}}{\tilde{b}} : \tilde{a} \in R,\ \tilde{b} \in \{\tilde{1}, \tilde{3}, \tilde{5}\}\}$. Es gilt:
$\frac{\tilde{a}}{\tilde{b}} = \frac{\tilde{0}}{\tilde{1}} \Leftrightarrow \exists\, \tilde{t} \in \{\tilde{1}, \tilde{3}, \tilde{5}\} :\ \tilde{t} \cdot (\tilde{a} \cdot \tilde{1} - \tilde{b} \cdot \tilde{0}) = \tilde{t} \cdot \tilde{a} = \tilde{0} \Leftrightarrow \tilde{a} \in I$
$\frac{\tilde{a}}{\tilde{b}} = \frac{\tilde{1}}{\tilde{1}} \Leftrightarrow \exists\, \tilde{t} \in \{\tilde{1}, \tilde{3}, \tilde{5}\} :\ \tilde{t} \cdot (\tilde{a} \cdot \tilde{1} - \tilde{b} \cdot \tilde{1}) = \tilde{t} \cdot (\tilde{a} - \tilde{b}) = \tilde{0} \Leftrightarrow \tilde{a} - \tilde{b} \in I \overset{\tilde{b} \notin I}{\Leftrightarrow} \tilde{a} \in \{\tilde{1}, \tilde{3}, \tilde{5}\}$
$\Rightarrow R_I = \{\frac{\tilde{0}}{\tilde{1}}, \frac{\tilde{1}}{\tilde{1}}\} \Rightarrow R_I \cong \mathbb{F}_2$ ist nullteilerfrei.
genauso: $R_J = \{\frac{\tilde{a}}{\tilde{b}} : \tilde{a} \in R,\ \tilde{b} \in \{\tilde{1}, \tilde{2}, \tilde{4}, \tilde{5}\}\} = \{\frac{\tilde{0}}{\tilde{1}}, \frac{\tilde{1}}{\tilde{1}}, \frac{\tilde{2}}{\tilde{1}}\} \cong \mathbb{F}_3$ ist nullteilerfrei.

Beachte:
Die beiden Lösungen stimmen überein, denn es ist $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{F}_2 \times \mathbb{F}_3$.

Aufgabe 4
Gegeben sei die Menge $R := \{a + \zeta b \,:\, a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$, wobei $\zeta = \frac{-1+\sqrt{3}i}{2}$ eine dritte Einheitswurzel ist.

a) Zeigen Sie, dass R ein kommutativer, nullteilerfreier Ring mit Eins ist.

b) Zeigen Sie, dass für jedes $r \in R$ die Norm

$$\varphi(r) := |r|^2 = r \cdot \overline{r}$$

eine ganze Zahl ist.

c) Bestimmen Sie die Einheiten von R.

d) Zeigen Sie, dass R ein euklidischer Ring ist.

Lösung:
$R = \{a + \zeta b \,:\, a, b \in \mathbb{Z}\} \subseteq \mathbb{C}, \quad \zeta = \frac{-1+\sqrt{3}i}{2}$
Es gilt $\zeta^2 + \zeta + 1 = 0$, da $X^2 + X + 1 = \frac{X^3-1}{X-1}$ das Minimalpolynom von ζ ist.

a) Seien $a, b, c, d \in \mathbb{Z}$.
$(a + \zeta b) - (c + \zeta d) = (a - c) + \zeta(b - d) \in R$
$(a + \zeta b) \cdot (c + \zeta d) = ac + \zeta(ad + bc) + \zeta^2 bd = ac + \zeta(ad + bc) + (-\zeta - 1)bd$
$= (ac - bd) + \zeta(ad + bc - bd) \in R$
$0 = 0 + \zeta \cdot 0 \in R$
$1 = 1 + \zeta \cdot 0 \in R$
$\Rightarrow R$ ist ein Teilring von $\mathbb{C}$ mit $0, 1 \in R$.
Da $\mathbb{C}$ kommutativ und nullteilerfrei ist, ist das auch R.
$\Rightarrow R$ ist ein kommutativer, nullteilerfreier Ring mit Eins.

b) Sei $r = a + \zeta b \in R$ mit $a, b \in \mathbb{Z}$.
$\Rightarrow \varphi(r) = r \cdot \overline{r} = (a + \zeta b) \cdot (a + \overline{\zeta} b) = (a + \zeta b) \cdot (a + \zeta^2 b) = a^2 + \zeta ab + \zeta^2 ab + \zeta^3 b^2$
$= a^2 + \zeta ab + (-\zeta - 1)ab + b^2 = a^2 - ab + b^2 \in \mathbb{Z}$
Beachte: Es gilt sogar $\varphi(r) \in \mathbb{N}$ wegen $\varphi(r) = |r|^2 \geq 0$.

c) $1 \cdot 1 = (-1) \cdot (-1) = 1$
$\zeta \cdot (-1 - \zeta) = \zeta \cdot \zeta^2 = \zeta^3 = 1$
$(-\zeta) \cdot (1 + \zeta) = (-\zeta) \cdot (-\zeta^2) = \zeta^3 = 1$
$\Rightarrow \{1, -1, \zeta, -\zeta, 1 + \zeta, -1 - \zeta\} \subseteq R^\times$
(Beachte: Das sind genau die sechsten Einheitswurzeln.)

Sei nun $r \in R$ eine Einheit. Schreibe $r = a + \zeta b$ mit geeigneten $a, b \in \mathbb{Z}$. Da r eine Einheit ist, gibt es ein $s \in R$ mit $rs = 1$.
$\Rightarrow \varphi(r) \cdot \varphi(s) = |r|^2 \cdot |s|^2 = |rs|^2 = |1|^2 = 1$
$\overset{\varphi(r), \varphi(s) \in \mathbb{N}}{\Rightarrow} \varphi(r) = \varphi(s) = 1 \overset{b)}{\Rightarrow} a^2 - ab + b^2 = 1$

- $b = 1 \Rightarrow a^2 - a + 1 = 1 \Rightarrow a \in \{0, 1\} \Rightarrow r \in \{\zeta, 1 + \zeta\}$
  $b = 0 \Rightarrow a^2 = 1 \Rightarrow a = \pm 1 \Rightarrow r \in \{1, -1\}$
  $b = -1 \Rightarrow a^2 + a + 1 = 1 \Rightarrow a \in \{0, -1\} \Rightarrow r \in \{-\zeta, -1 - \zeta\}$

- Wäre $|b| \geq 2$, so wäre $1 = a^2 - ab + b^2 = (a - \frac{b}{2})^2 + \frac{3}{4}b^2 \geq 0 + \frac{3}{4} \cdot 4 = 3$, d.h. der Fall $|b| \geq 2$ kommt nicht vor.

Insgesamt erhalten wir $R^\times = \{1, -1, \zeta, -\zeta, 1+\zeta, -1-\zeta\}$.

d) Es gilt $\varphi(r) = 0 \Leftrightarrow |r|^2 = 0 \Leftrightarrow r = 0$.
$\Rightarrow \varphi$ ist eine Abbildung $\varphi : R \setminus \{0\} \to \mathbb{N}_{\geq 1}$.
Beh.: (R, φ) ist ein euklidischer Ring.

Seien $a, b, c, d \in \mathbb{Z}$ mit $a + \zeta b \in R$ und $c + \zeta d \in R \setminus \{0\}$.
$\Rightarrow \frac{a+\zeta b}{c+\zeta d} \in \mathbb{C}$
$\Rightarrow$ Es gibt $\tilde{x}, \tilde{y} \in \mathbb{R}$ mit $\frac{a+\zeta b}{c+\zeta d} = \tilde{x} + \zeta\tilde{y}$.
(Beachte: $\{1, \zeta\}$ ist $\mathbb{R}$-linear unabhängig, also eine Basis des $\mathbb{R}$-Vektorraums $\mathbb{C}$.)
Es gibt $x, y \in \mathbb{Z}$ mit $|\tilde{x} - x| \leq \frac{1}{2}$ und $|\tilde{y} - y| \leq \frac{1}{2}$.

Seien $q := x + \zeta y$ und $r := (a + \zeta b) - q \cdot (c + \zeta d)$. Damit haben wir $(a + \zeta b) = q \cdot (c + \zeta d) + r$. Außerdem gilt:

$$\begin{aligned}
\varphi(r) &= |(a+\zeta b) - q\cdot(c+\zeta d)|^2 = |c+\zeta d|^2 \cdot \left|\tfrac{a+\zeta b}{c+\zeta d} - q\right|^2 = \varphi(c+\zeta d)\cdot|(\tilde{x}+\zeta\tilde{y}) - (x+\zeta y)|^2 \\
&= \varphi(c+\zeta d)\cdot|(\tilde{x}-x) + \zeta(\tilde{y}-y)|^2 \leq \varphi(c+\zeta d)\cdot(|\tilde{x}-x|^2 + |\zeta|^2|\tilde{y}-y|^2) \\
&= \varphi(c+\zeta d)\cdot(|\tilde{x}-x|^2 + |\tilde{y}-y|^2) \leq \varphi(c+\zeta d)\cdot(\tfrac{1}{4}+\tfrac{1}{4}) = \tfrac{1}{2}\cdot\varphi(c+\zeta d) \\
&< \varphi(c+\zeta d)
\end{aligned}$$

Aufgabe 5
Es seien $\mathbb{F}_3$ und $\mathbb{F}_9$ die Körper mit 3 bzw. 9 Elementen. Bestimmen Sie für jedes Element $x \in \mathbb{F}_9 \setminus \{0\}$ das Minimalpolynom von x über $\mathbb{F}_3$ sowie die Ordnung von x in $\mathbb{F}_9^\times$.

Lösung:
$\mathbb{F}_3 = \{0, 1, 2\}$, $\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2+1)$
(Beachte: X^2+1 ist irreduzibel in $\mathbb{F}_3[X]$.)
$\Rightarrow \mathbb{F}_9 = \{\overline{0}, \overline{1}, \overline{2}, \overline{X}, \overline{X+1}, \overline{X+2}, \overline{2X}, \overline{2X+1}, \overline{2X+2}\}$

- $(\overline{X+1})^1 = \overline{X+1}$
  $(\overline{X+1})^2 = \overline{(X+1)(X+1)} \overset{\overline{X^2}=\overline{-1}=2}{=} \overline{2+2X+1} = \overline{2X}$
  $(\overline{X+1})^3 = \overline{(2X)(X+1)} = \overline{2X+1}$
  $(\overline{X+1})^4 = \overline{(2X)(2X)} = \overline{2}$
  $(\overline{X+1})^5 = \overline{2(X+1)} = \overline{2X+2}$
  $(\overline{X+1})^6 = \overline{2(2X)} = \overline{X}$
  $(\overline{X+1})^7 = \overline{X(X+1)} = \overline{X+2}$
  $(\overline{X+1})^8 = \overline{2 \cdot 2} = \overline{1}$
  Hieraus liest man ab:
  $\operatorname{ord}(\overline{1}) = 1$, $\operatorname{ord}(\overline{2}) = 2$, $\operatorname{ord}(\overline{X}) = \operatorname{ord}(\overline{2X}) = 4$,
  $\operatorname{ord}(\overline{X+1}) = \operatorname{ord}(\overline{X+2}) = \operatorname{ord}(\overline{2X+1}) = \operatorname{ord}(\overline{2X+2}) = 8$

- Die Elemente von $\mathbb{F}_9$ sind die Nullstellen des Polynoms $T^9 - T \in \mathbb{F}_3[T]$. Es gilt:
  $T^9 - T = T \cdot (T^8 - 1) = T \cdot (T^4 - 1) \cdot (T^4 + 1) = T \cdot (T^2 - 1) \cdot (T^2 + 1) \cdot (T^4 + 1)$
  $= T \cdot (T - 1) \cdot (T + 1) \cdot (T^2 + 1) \cdot (T^4 + 1)$
  $= T \cdot (T - 1) \cdot (T + 1) \cdot (T^2 + 1) \cdot (T^2 + T - 1) \cdot (T^2 - T - 1)$
  Die Faktoren in der letzten Zeile sind alle irreduzibel und normiert. (Sie müssen irreduzibel sein, da $T^9 - T$ separabel ist und alle linearen Terme vorkommen.)

- Das Minimalpolynom von $\overline{0}$ ist T.
  Das Minimalpolynom von $\overline{1}$ ist $T - 1$.
  Das Minimalpolynom von $\overline{2}$ ist $T + 1$.
  $\overline{X}^2 + \overline{1} = \overline{X^2 + 1} = \overline{0} \Rightarrow$ Das Minimalpolynom von $\overline{X}$ ist $T^2 + 1$.
  $\overline{2X}^2 + \overline{1} = \overline{4X^2 + 1} = \overline{0} \Rightarrow$ Das Minimalpolynom von $\overline{2X}$ ist $T^2 + 1$.
  $\overline{X+1}^2 + \overline{X+1} - \overline{1} = \overline{2X + X + 1 - 1} = \overline{0} \Rightarrow$ Das Minimalpolynom von $\overline{X+1}$ ist $T^2 + T - 1$.
  $\overline{2X+1}^2 + \overline{2X+1} - \overline{1} = \ldots = \overline{0} \Rightarrow$ Das Minimalpolynom von $\overline{2X+1}$ ist $T^2 + T - 1$.
  $\Rightarrow$ Das Minimalpolynom von $\overline{X+2}$ und von $\overline{2X+2}$ ist jeweils $T^2 - T - 1$.

Aufgabe 6
Gegeben sei das rationale Polynom $f = X^4 - 2X^2 - 3 \in \mathbb{Q}[X]$.

a) Bestimmen Sie die Galoisgruppe $\mathrm{Gal}(f)$ von f, alle Untergruppen von $\mathrm{Gal}(f)$ und die zugehörigen Fixkörper.

b) Geben Sie eine Körperkette $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_m = Z(f)$ von elementaren Radikalerweiterungen an. Dabei sei $Z(f)$ ein Zerfällungskörper von f.

Lösung:

a) $f = X^4 - 2X^2 - 3 = (X^2 - 3)(X^2 + 1)$
f hat die komplexen Nullstellen $\sqrt{3}, -\sqrt{3}, i, -i$.
$\Rightarrow Z(f) = \mathbb{Q}(\sqrt{3}, -\sqrt{3}, i, -i) = \mathbb{Q}(\sqrt{3}, i)$
Wegen $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{3}) \subsetneq \mathbb{Q}(\sqrt{3}, i)$ ist $[Z(f) : \mathbb{Q}] = 4$.
$\Rightarrow |\mathrm{Gal}(f)| = 4$

Jeder Automorphismus $\sigma \in \mathrm{Gal}(f) = \mathrm{Aut}(\mathbb{Q}(\sqrt{3}, i))$ ist durch die Angabe der Bilder von $\sqrt{3}$ und i eindeutig bestimmt. Dabei kann $\sqrt{3}$ auf $\sqrt{3}$ oder $-\sqrt{3}$ abgebildet werden, und i kann auf i oder $-i$ abgebildet werden.
$\Rightarrow \mathrm{Gal}(f) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ mit:

$$\begin{aligned} \sigma_1(i) &= i, & \sigma_1(\sqrt{3}) &= \sqrt{3}, \\ \sigma_2(i) &= i, & \sigma_2(\sqrt{3}) &= -\sqrt{3}, \\ \sigma_3(i) &= -i, & \sigma_3(\sqrt{3}) &= \sqrt{3}, \\ \sigma_4(i) &= -i, & \sigma_4(\sqrt{3}) &= -\sqrt{3}. \end{aligned}$$

(Beachte: Es ist $\sigma_1 = \mathrm{id}$.)
Für jedes $n = 1, \ldots, 4$ gilt $\sigma_n^2(i) = \sigma_n(\pm i) = \pm\sigma_n(i) = \pm(\pm i) = i$ und $\sigma_n^2(\sqrt{3}) = \sigma_n(\pm\sqrt{3}) = \pm\sigma_n(\sqrt{3}) = \pm(\pm\sqrt{3}) = \sqrt{3}$, also $\sigma_n^2 = \mathrm{id}$.
$\Rightarrow \mathrm{Gal}(f) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$\Rightarrow$ Die Untergruppen von $\mathrm{Gal}(f)$ sind $\{\sigma_1\}$, $\{\sigma_1, \sigma_2\}$, $\{\sigma_1, \sigma_3\}$, $\{\sigma_1, \sigma_4\}$ und $\mathrm{Gal}(f)$.

Die zugehörigen Fixkörper sind:
$Z(f)^{\{\sigma_1\}} = \{x \in \mathbb{Q}(\sqrt{3}, i) \,:\, \sigma_1(x) = x\} = \mathbb{Q}(\sqrt{3}, i)$
$Z(f)^{\{\sigma_1, \sigma_2\}} = \{x \in \mathbb{Q}(\sqrt{3}, i) \,:\, \sigma_1(x) = \sigma_2(x) = x\} = \mathbb{Q}(i)$
$Z(f)^{\{\sigma_1, \sigma_3\}} = \{x \in \mathbb{Q}(\sqrt{3}, i) \,:\, \sigma_1(x) = \sigma_3(x) = x\} = \mathbb{Q}(\sqrt{3})$
$Z(f)^{\{\sigma_1, \sigma_4\}} = \{x \in \mathbb{Q}(\sqrt{3}, i) \,:\, \sigma_1(x) = \sigma_4(x) = x\} = \mathbb{Q}(\sqrt{3}i)$
$Z(f)^{\mathrm{Gal}(f)} \overset{\text{Hauptsatz}}{=} \mathbb{Q}$

Exemplarisch rechnen wir das für die Untergruppe $\{\sigma_1, \sigma_2\}$ nach:
Sei $x = a + bi + c\sqrt{3} + d\sqrt{3}i \in \mathbb{Q}(\sqrt{3}, i)$ mit $a, b, c, d \in \mathbb{Q}$. Dann gilt:

$$\begin{aligned} x \in Z(f)^{\{\sigma_1, \sigma_2\}} &\Leftrightarrow \sigma_1(x) = \sigma_2(x) = x \Leftrightarrow \sigma_2(x) = x \\ &\Leftrightarrow a + bi - c\sqrt{3} - d\sqrt{3}i = a + bi + c\sqrt{3} + d\sqrt{3}i \Leftrightarrow 2\sqrt{3}(c + di) = 0 \\ &\Leftrightarrow c + di = 0 \Leftrightarrow c = d = 0 \\ &\Leftrightarrow x = a + bi \in \mathbb{Q}(i) \end{aligned}$$

b) Die Körperkette $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{3}, i) = Z(f)$ leistet das Gewünschte, denn die Körpererweiterungen $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ und $\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q}(\sqrt{3})$ sind Zerfällungskörper der Polynome $X^2 - 3$ bzw. $X^2 + 1$.