Aufgabe 1 (12 Punkte). (a) Geben Sie die Definition einer *auflösbaren Gruppe* an.

(b) Sei $d \geqslant 1$ eine natürliche Zahl. Geben Sie eine Definition für das d-te *Kreisteilungspolynom* $\phi_d(X)$ über den rationalen Zahlen an.

(c) Geben Sie eine Formulierung des *Satzes vom primitiven Element* an.

Lösung. **Zu (a):** Eine Gruppe G heißt auflösbar, wenn folgende äquivalente Bedingungen erfüllt sind:

(a) Es gibt $n \in \mathbb{N}_0$ mit $D^n(G) = \{e\}$.

(b) Es gibt eine Folge von Normalteilern $G = H_0 \supset H_1 \supset \ldots \supset H_m = \{e\}$, $m \geqslant 0$, so daß H_i/H_{i+1} abelsch ist für $0 \leqslant i < m$.

(c) Es gibt eine Folge von Untergruppen $G = H_0 \supset H_1 \supset \ldots \supset H_m = \{e\}$, $m \geqslant 0$, so daß $H_{i+1} \triangleleft H_i$ und H_i/H_{i+1} abelsch ist für $0 \leqslant i < m$.

Zu (b): Es sei $\mathbb{Q}^{(d)}$ ein Zerfällungskörper des Polynoms $X^d - 1 \in \mathbb{Q}[X]$ und P_d die Menge aller primitiven d^{ten} Einheitswurzeln in $\mathbb{Q}^{(d)}$. Das Polynom $\phi_{\mathbb{Q},d} = \phi_d = \prod_{\zeta \in P_d}(X - \zeta)$ ist das d-te Kreisteilungspolynom über $\mathbb{Q}$.

Zu (c): Jede endliche separabel Erweiterung $K \subset L$ ist einfach, dh. es gibt $x \in L$ mit $L = K(x)$.

Aufgabe 2 (12 Punkte). (a) Geben Sie ein normiertes Polynom mit rationalen Koeffizienten an, welches $\sqrt{2} + \sqrt{7}$ als Nullstelle hat.

(b) Mit S_n wollen wir die symmetrischen, mit A_n die alternierenden Gruppen bezeichnen. Begründen Sie, warum $A_3 \times A_3$ die einzige 3-Sylowgruppe von $S_3 \times S_3$ ist.

(c) Sei $f(X) = X^2 + pX + q$ ein Polynom mit rationalen Koeffizienten. Was können Sie über die Galoissche Gruppe von $f(X)$ sagen, wenn die Diskriminante $\Delta := p^2 - 4q$ ein Quadrat in den rationalen Zahlen ist?

Lösung. **Zu (a):** Man rechnet leicht nach, daß

$$X^4 - 18X^2 + 25 \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$$

ein solches Polynom ist (sogar das Minimalpolynom).

Zu (b): Die Ordnung von $S_3 \times S_3$ ist

$$|S_3 \times S_3| = |S_3| \cdot |S_3| = 3! \cdot 3! = 3^2 \cdot 2^2.$$

Also hat jede 3-Sylowuntergruppe Ordnung 3^2. Eine solche existiert nach dem ersten der Sylowsätze. Wir wissen, daß die alternierende Gruppe $A_3 \subset S_3$ Index 2 hat, hat also Ordnung 3. Es folgt, daß $A_3 \times A_3$ die Ordnung

$$|A_3 \times A_3| = |A_3| \cdot |A_3| = 3^2$$

hatalso eine 3-Sylowuntergruppe von $S_3 \times S_3$ ist.
Da außerdem A_3 Normalteiler in S_3 ist, und in $S_3 \times S_3$ die Multiplikation komponentenweise definiert ist, prüft man leicht nach, daß $A_3 \times A_3$ Normalteiler in $S_3 \times S_3$ ist. Damit ist $A_3 \times A_3$ die einzige 3-Sylowuntergruppe.

Zu (c): Die Galoisgruppe $G(f)$ von f über $\mathbb{Q}$ ist nach Definition die Galoisgruppe eines Zerfällungskörpers von f über $\mathbb{Q}$. Da f den Grad 2 hat, gibt es einen Monomorphismus $\varphi : G(f) \to S_2 \cong \mathbb{Z}/2\mathbb{Z}$. Sei $G(f)_+ = \varphi^{-1}(A_2)$. Es gilt $A_2 = \{\mathrm{id}\} \cong \{0\}$. Also ist $G(f)_+ = \{\mathrm{id}\}$ trivial. Im allgemeinen gilt genau dann $G(f) = G(f)_+$ wenn $\Delta(f)$ ein Quadrat in $\mathbb{Q}$ ist, was hier der Fall ist. Dies zeigt, daß hier die Galoisgruppe von f trivial ist.

Aufgabe 3 (12 Punkte)**.** Mit $\mathbb{Q}$ bezeichnen wir den Körper der rationalen Zahlen.
Sei $f(X)$ ein irreduzibles Polynom fünften Grades über den rationalen Zahlen, dessen galoissche Gruppe isomorph zur symmetrischen Gruppe S_5 ist. Mit L bezeichnen wir einen Zerfällungskörper von $f(X)$ über den rationalen Zahlen.

(a) Welchen Grad hat L über $\mathbb{Q}$? (Geben Sie eine kurze Begründung an.)

(b) Seien $x_1, \ldots, x_5$ die Nullstellen von $f(X)$ in L. Kann der Fall $x_i = x_j$ mit $i \neq j$ auftreten? (Geben Sie eine kurze Begründung an.)

(c) Für jedes $i = 0, \ldots, 5$ betrachten wir die Zwischenerweiterung $K_i = \mathbb{Q}(x_1, \ldots, x_i)$ (das heißt indbesondere $K_0 = \mathbb{Q}$) von L über $\mathbb{Q}$. Bestimmen Sie den Grad von K_{i+1} über K_i für $i = 0, \ldots, 4$.

(d) Geben Sie eine Begründung dafür an, warum $f(X)$ über $\mathbb{Q}$ nicht, dafür aber über K_1 auflösbar ist.

Lösung. **Zu (a):** Da $\operatorname{char}(\mathbb{Q}) = 0$ ist, ist $\mathbb{Q}$ vollkommen, also jedes irreduzible Polynom über $\mathbb{Q}$ separabel. Insbesondere ist f separabel. Also ist L Zerfällungskörper eines separablen Polynoms, anders gesagt, L ist eine eindliche Galoiserweiterung von $\mathbb{Q}$. Für solche gilt

$$[L : \mathbb{Q}] = |\operatorname{Gal}(L/\mathbb{Q})| = 5! = 120.$$

Zu (b): Nein. Wie schon festgestellt ist f ein irreduzibles separables Polynom. Ein solches hat nach Definition in einem (und dann jedem) Zerfällungskörper nur einfache Nullstellen.

Zu (c): Als Zerfällungskörper von f ist $L = K_5 = \mathbb{Q}(x_1, x_2, x_3, x_4, x_5)$, und das Polynom f zerfällt in L in Linearfaktoren

$$f = (X - x_1)(X - x_2)(X - x_3)(X - x_4)(X - x_5),$$

Es ist irreduzibel über $\mathbb{Q}$. Da x_1 eine Nullstelle ist, ist es das Minimalpolynom von x_1 über $\mathbb{Q}$, und es gilt

$$[K_1 : K_0] = [\mathbb{Q}(x_1) : \mathbb{Q}] = \deg(f) = 5.$$

Da $f, X - x_1 \in \mathbb{Q}(x_1)[X]$, ist

$$g = (X - x_2)(X - x_3)(X - x_4)(X - x_5) = \frac{f}{X - x_1} \in \mathbb{Q}(x_1)[X].$$

Da x_2 Nullstelle von g ist, teilt das Minimalpolynom von x_2 über $\mathbb{Q}(x_1)$ g. Also hat dieses maximal Grad 4, und

$$[K_2 : K_1] = [\mathbb{Q}(x_1, x_2) : \mathbb{Q}(x_1)] \leqslant 4.$$

Ebenso ist

$$h = (X - x_3)(X - x_4)(X - x_5) = \frac{f}{(X - x_1)(X - x_2)} \in \mathbb{Q}(x_1, x_2)[X].$$

Da x_3 Nullstelle von h ist, teilt das Minimalpolynom on x_3 über $\mathbb{Q}(x_1, x_2)$ h. Also hat dieses maximal Grad 3, und

$$[K_3 : K_2] = [\mathbb{Q}(x_1, x_2, x_3) : \mathbb{Q}(x_1, x_2)] \leqslant 3.$$

Weiter ist

$$e = (X - x_4)(X - x_5) = \frac{f}{(X - x_1)(X - x_2)(X - x_3)} \in \mathbb{Q}(x_1, x_2, x_3)[X].$$

Da x_4 Nullstelle von e ist, teilt das Minimalpolynom on x_4 über $\mathbb{Q}(x_1, x_2, x_3)$ e. Also hat dieses maximal Grad 2, und

$$[K_4 : K_3] = [\mathbb{Q}(x_1, x_2, x_3, x_4) : \mathbb{Q}(x_1, x_2, x_3)] \leqslant 2.$$

Nun ist,

$$(X - x_5) = \frac{f}{(X - x_1)(X - x_2)(X - x_3)(X - x_4)} \in \mathbb{Q}(x_1, x_2, x_3, x_4)[X],$$

also $x_5 \in \mathbb{Q}(x_1, x_2, x_3, x_4)$, also $\mathbb{Q}(x_1, x_2, x_3, x_4, x_5) = \mathbb{Q}(x_1, x_2, x_3, x_4)$, und damit

$$[K_5 : K_4] = [\mathbb{Q}(x_1, x_2, x_3, x_4, x_5) : \mathbb{Q}(x_1, x_2, x_3, x_4)] = 1.$$

Durch vierfache Anwendung des Gradsatzes erhält man

$$[L:\mathbb{Q}] = [K_5 : K_4] \cdot [K_4 : K_3] \cdot [K_3 : K_2] \cdot [K_2 : K_1] \cdot [K_1 : K_0].$$

Da $[L : \mathbb{Q}] = 5!$ müssen alle Ungleichungen von oben also Gleichungen sein, und man erhält

$$[K_{i+1} : K[i] = 5 - i.$$

Zu (d): Ein Polynom ist genau dann auflösbar, wenn die zugehörige Galoisgruppe auflösbar ist. Die Galoisgruppe $G_{\mathbb{Q}}(f)$ von f über $\mathbb{Q}$ ist S_5, eine nicht-auflösbare Gruppe. Wie wir in **(c)** gesehen haben, ist $[K_1 : \mathbb{Q}] = 5$, also nach dem Gradsatz

$$[L : K_1] = \frac{[L:\mathbb{Q}]}{[K_1 : \mathbb{Q}]} = 4!.$$

Insbesondere ist L Zerfällungskörper nicht nur Zerfällungskörper von f über K_1 sondern auch von $g = (X - x_2)(X - x_3)(X - x_4)(X - x_5)$ über K_1 und es gilt $G_{K_1}(f) = G_{K_1}(g)$. Da g Polynom vierten Grades ist, ist diese eine Untergruppe von S_4, aus Gradgründen sogar gleich S_4. Da S_4 auflösbar ist, ist f auflösbar über K_1.

Aufgabe 4 (12 Punkte)**.** Zur Erinnerung: Eine komplexe Zahl heißt *algebraisch*, wenn sie Nullstelle eines Polynoms mit rationalen Koeffizienten ist.

(a) Sei $n \geqslant 1$ eine natürliche Zahl und sei $c \in \mathbb{C}^n$ ein nicht verschwindender Vektor aus komplexen Zahlen. Zeigen Sie, daß eine komplexe Zahl z algebraisch ist, wenn eine rationale $n \times n$-Matrix mit

$$z \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = A \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$$

existiert.
(Hinweis: Betrachten Sie das charakteristische Polynom von A.)

(b) Seien x und y zwei algebraische Zahlen. Benutzen Sie die Aussage aus dem ersten Aufgabenteil, um zu zeigen, daß $z = x + y$ ebenfalls algebraisch ist.
(Hinweis: Betrachten Sie einen Vektor c, dessen Einträge von der Form $x^i y^j$ sind.)

Lösung. **Zu (a):** Angenommen es gibt A und c wie angegeben. Das heißt, daß $0 \neq c \in \mathbb{C}^n$ ein nicht-trivialer Eigenvektor der rationalen Matrix A zum Eigenwert x ist. Insbesonder ist x Nullstelle des charakteristischen Polynoms $\chi_A \in \mathbb{Q}[X]$ von A. Dieses hat rationale Koeffizienten, da die Matrix A rationale Einträge hat. Also ist x algebraisch.

Zu (b): Sei n der Grad des Minimalpolynoms f von x über $\mathbb{Q}$ und m der Grad des Minimalpolynoms g von y über $\mathbb{Q}$. Wir betrachten einen Vektor $c \in \mathbb{C}^{n+m}$ mit den Einträgen $x^i y^j$, $0 \leqslant i \leqslant n-1$, $0 \leqslant j \leqslant m-1$, in beliebiger Ordnung.
Wir müssen nun eine $(n + m) \times (n + m)$ Matrix A identifizieren mit $Ac = zc$. Sei $x^i y^j$ der r-te Eintrag von c für ein $1 \leqslant r \leqslant n + m$.Dann ist der r-te Eintrag von zc gegeben durch $x^{i+1}y^j + x^i y^{j+1}$. Wir werden nun die Einträge in der r-ten Reihe von A identifizieren.
1. Fall – $i < n - 1$, $j < m - 1$: Dann sind auch $x^{i+1}y^j$ und $x^i y^{j+1}$ Einträge in c, und wir wählen für die dazu gehörenden Einträge in der r-ten Reihe von A jeweils 1, und setzen die restlichen Einträge $= 0$.
2. Fall – $i = n - 1$, $j < m - 1$: Da $f(x) = 0$, normiert ist, und $\deg(f) = n$ folgt $x^n = x^n - f(x) =: s(x)$ und dies ist ein Polynom über $\mathbb{Q}$ vom Grad $n - 1$. Das heißt wir können x^n als Linearkombination der $1, \ldots, x^{n-1}$ ausdrücken, und $x^n y^j = s(x)y^j$ ist eine Darstellung als Linearkombination in $y^j, \ldots, x^{n-1}y^j$. Die Koeffizienten diese Ausdrucks wählen wir als Einträge der r-ten Reihe von A zusammen mit dem Eintrag 1 für die zu $x^{n-1}y^{j+1}$ gehörende Stelle und Nullen für den Rest.
3. Fall – $i < n - 1$, $j = m - 1$: Wie im Fall 2 mit i und j vertauscht.
4. Fall – $i = n - 1$, $j = m - 1$: Die Kombination vom Fall 3 und 4, wobei die Einträge der r-ten Reihe von A anhand der Minimalpolynome von x und y identifizieren.
Wir erhalten so eine rationale Matrix A mit $Ac = xc$.

Aufgabe 5 (12 Punkte). (a) Sei $\mathbb{Z}$ der Ring der ganzen Zahlen. Zeigen Sie, daß der Ring $\mathbb{Z}[i]/(2)$ (wobei $i^2 = -1$) genau vier Elemente hat.

(b) Sei R ein kommutativer Ring mit 1. Sei weiter $t \in R$. Zeigen Sie, daß jedes Element im Quotientenring $R[X]/(tX-1)$ kongruent zu einem Element der Form aX^n modulo $tX-1$ ist, wobei $a \in R$ und $n \geqslant 1$ eine natürliche Zahl ist.

(c) Für einen kommutativen Ring R mit 1 wollen wir mit $\mathrm{Spec}(R)$ die Menge der Primideale von R bezeichnen. Sei $\phi : R \to S$ ein Ringhomomorphismus in einen weiteren kommutativen Ring mit 1. Geben Sie einen Beweis dafür an, daß

$$\phi^{-1} : \mathrm{Spec}(S) \to \mathrm{Spec}(R), \mathfrak{p} \mapsto \phi^{-1}(\mathfrak{p})$$

eine wohldefinierte Abbildung ist.

Lösung. **Zu (a):** Da $\mathbb{Z}[i]$ kommutativ ist, gilt das gleiche für $\mathbb{Z}[i]/(2)$. Wir zeigen, daß die additive Gruppe von $\mathbb{Z}[i]/(2)$ isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ist. Betrachte den Gruppenhomomorphismus

$$\varphi : \mathbb{Z}[i] \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, a + bi \mapsto (\overline{a}, \overline{b}).$$

Dieser ist wohldefiniert und surjektiv. Sein Kern ist das von 2 erzeugte Ideal: Es ist klar, daß $\varphi(2) = (\overline{0}, \overline{0})$, also $(2) \subset \ker(\varphi)$. Ist andererseits $\varphi(a + bi) = (\overline{a}, \overline{b}) = (\overline{0}, \overline{0})$, so ist $a \equiv 0 \mod 2$ und $b \equiv 0 \mod 2$ in $\mathbb{Z}$. Also ist $a + bi$ ein Vielfaches von 2 und damit $(2) = \ker(\varphi)$.
Nach einem der Homomorphiesätze für Gruppen ist $\mathbb{Z}[i]/(2) \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2)$, und letzteres hat vier Elemente.
(Es spielt hier keine Rolle, daß die Multiplikation nicht komponentenweise definiert ist.

Zu (b): Sei $f \in R[X]$ ein Polynom und $\deg(f) = n$. Wir zeigen durch Induktion nach n daß f in $R[X]/(tX-1)$ entweder einen Represäntanten der Form aX^n (mit dem gleichen n) hat, oder verschwindet. Sei $n = 0$, dann ist $f = a_0$ konstant, und die Aussage gilt trivialerweise. Sei $n = 1$, dann ist f von der Form $f = r_1X + r_0$, und für die Nebeklasse von f modulo dem Ideal $(tX - 1)_R$ gilt

$$\begin{aligned}\overline{f} &= r_1X + r_0 + (tX-1)_R \\ &= r_1X + r_0 + r_0(tX-1) + (tX-1)_R \\ &= (r_1 + r_0t)X + (tX-1)_R\end{aligned}$$

und $\overline{f}$ hat einen Represäntanten der gewünschten Form, welcher genau dann trivial ist, wenn $r_1 = -r_0t$.
Es sei die Aussage für $n \geqslant 1$ bereits gezeigt. Sei $f = r_{n+1}X^{n+1} + r_nX^n + \ldots + r_1X + r_0 \in R[X]$ ein Polynom vom Grad $n+1$. Nach Induktionsvoraussetzung ist $g := r_nX^n + \ldots + r_1X + r_0$ entweder in $(tX-1)_R$ enthalten (dann ist $\overline{g} = \overline{0}$, oder es hat einen Represäntanten der Form aX^n. Im ersten Fall sind wir fertig, denn dann ist $r_{n+1}X^{n+1}$ ein Represäntant von f modulo $(tX-1)_R$. Andernfalls berechnen wir

$$\begin{aligned}\overline{f} &= r_{n+1}X^{n+1} + r_nX^n + \ldots + r_1X + r_0 + (tX-1)_R \\ &= r_{n+1}X^{n+1} + aX^n + (tX-1)_R \\ &= r_{n+1}X^{n+1} + aX^n + aX^n(tX-1) + (tX-1)_R \\ &= (r_{n+1} + at)X^{n+1} + (tX-1)_R\end{aligned}$$

und $\overline{f}$ hat einen Represäntanten der gewünschten Form, welcher genau dann trivial ist, wenn $r_{n+1} = -at$.

Zu (c): Um zu zeigen, daß die Abbildung wohldefiniert ist, genügt es zu zeigen, daß das Urbild $\phi^{-1}(\mathfrak{p})$ eines Primideals $\mathfrak{p}$ in S unter dem Ringhomomorphismus ϕ ein Primideal in R ist.
Es ist klar, daß Urbilder von Idealen wieder Ideale sind. Wegen $1 \notin \mathfrak{p}$, gilt $1 \notin \phi^{-1}(\mathfrak{p})$. Seien $r, r' \in R$ mit $rr' \in \phi^{-1}(\mathfrak{p})$. Dann ist $\phi(r)\phi(r') = \phi(rr') \in \mathfrak{p}$. Also ist $\phi(r) \in \mathfrak{p}$ oder $\phi(r') \in \mathfrak{p}$. Damit ist $r \in \phi^{-1}(\mathfrak{p})$ oder $r' \in \phi^{-1}(\mathfrak{p})$. Dies zeigt, daß $\phi^{-1}(\mathfrak{p})$ ein Primideal ist.