Thema Nr. 3
(Aufgabengruppe)

Es sind alle Aufgaben dieser Aufgabengruppe zu bearbeiten!

Aufgabe 1 (12 Punkte)

Sei G eine Gruppe und H eine Untergruppe von G.

(a) Geben Sie die Definition des *Index* $(G : H)$ an. (G muss nicht endlich sein.)

(b) Zeigen Sie, dass $(G : H)$ ein Teiler von 168 ist, wenn H der Kern eines Homomorphismus $f\colon G \to \mathrm{GL}_3(\mathbb{F}_2)$ in die Gruppe der invertierbaren 3×3-Matrizen über dem Körper $\mathbb{F}_2$ ist.

Aufgabe 2 (12 Punkte)

Es seien $\alpha := \sqrt{\sqrt{12}+3} \in \mathbb{R}$, $\beta := i\sqrt{\sqrt{12}-3} \in \mathbb{C}$ und $L := \mathbb{Q}(\alpha, \beta) \subseteq \mathbb{C}$.

(a) Bestimmen Sie das Minimalpolynom $f = m_{\alpha,\mathbb{Q}}$ von α über $\mathbb{Q}$ und zeigen Sie, dass auch β eine Nullstelle von f ist.

(b) Begründen Sie, warum $L/\mathbb{Q}$ eine Galois-Erweiterung ist.

(c) Zeigen Sie, dass $L = \mathbb{Q}(\alpha, i)$ gilt, und bestimmen Sie den Grad $[L : \mathbb{Q}]$.

(d) Zeigen Sie, dass die Galois-Gruppe $\mathrm{Gal}(L/\mathbb{Q})$ einen Normalteiler der Ordnung 2 enthält.

Aufgabe 3 (12 Punkte)

Sei L Zerfällungskörper des Polynoms $f := X^4 - X^3 + 2X^2 - 2$ über $\mathbb{Q}$. Bestimmen Sie

(a) für eine Nullstelle $1 \neq \alpha \in L$ von f das Minimalpolynom von α über $\mathbb{Q}$,

(b) den Grad $[L : \mathbb{Q}]$.

Aufgabe 4 (12 Punkte)

(a) Seien p eine ungerade Primzahl und $n \geq 1$. Zeigen Sie, dass die Gleichung $x^2 = 1$ in $R = \mathbb{Z}/p^n\mathbb{Z}$ genau zwei Lösungen hat.

(b) Bestimmen Sie alle Lösungen der Gleichung $x^2 = 1$ im Ring $\mathbb{Z}/2023\mathbb{Z}$.
Hinweis: $2023 = 7 \cdot 17^2$.

Aufgabe 5 (12 Punkte)

Seien $R \neq 0$ ein kommutativer Ring und $F, G \in R[X]$ Polynome, wobei G als normiert angenommen sei. Dann (das sollen Sie nicht beweisen) existieren eindeutig bestimmte $A, B \in R[X]$ so, dass gelten $F = AG + B$ und $\deg(B) < \deg(G)$ (hierbei ist $\deg(0) := -\infty$). (Das ist Division mit Rest durch ein normiertes Polynom).

(a) Seien $f\colon R \to S \neq 0$ ein Ringhomomorphismus und $f[X]\colon R[X] \to S[X]$ der Ringhomomorphismus, der auf $R \subseteq R[X]$ mit f übereinstimmt und außerdem $f[X](X) = X$ erfüllt. Zeigen Sie, dass in $S[X]$ gilt $f[X](F) = f[X](A) \cdot f[X](G) + f[X](B)$, und dass diese Gleichung die Division mit Rest von $f[X](F)$ durch $f[X](G)$ ist.

(b) Zeigen Sie, dass genau ein Ideal $I \subseteq R$ existiert, sodass für jeden Ringhomomorphismus $f\colon R \to S \neq 0$ äquivalent sind:

(i) $f[X](G)$ teilt $f[X](F)$ in $S[X]$.

(ii) $f(I) = 0$.

(c) Bestimmen Sie das Ideal $I \subseteq R$ aus Teil (b) in den beiden folgenden Fällen:

(i) $R := \mathbb{Z}, \quad F := X^3 - 1, \quad G := X^2 + 1 \in R[X]$.

(ii) $R := \mathbb{Z}[Y], \quad F(X) := X^2 + Y, \quad G(X) := X - 1 \in R[X]$.