Aufgabe 1 (20 Punkte) | I | II | **Seite 1**

Im Folgenden finden Sie 5 Aussagen ((a)-(e)), die richtig oder falsch sein können. Kreuzen Sie bitte jeweils Zutreffendes an und begründen Sie Ihre Wahl.

(a) Es gibt einen Gruppenhomomorphismus $\psi : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$ mit $\psi(1+2\mathbb{Z}) \neq 0$.

(b) Ist $K \supset k$ algebraisch, so folgt $[K : k] < \infty$.

(c) Es gibt einen Ringisomorphismus $\mathbb{F}_4 \to \mathbb{Z}/4\mathbb{Z}$.

(d) Die Zahl $\sqrt[3]{5}$ ist nicht mit Zirkel und Lineal konstruierbar.

(e) Es gibt einen Körper mit 6 Elementen.

Lösung:

(a) FALSCH. Es ist $0 = \psi(0+2\mathbb{Z}) = \psi(1+2\mathbb{Z}+1+2\mathbb{Z}) = \psi(1+2\mathbb{Z}) + \psi(1+2\mathbb{Z})$. In $(\mathbb{Z},+)$ gibt es aber bekanntlich kein Element $\psi(1+2\mathbb{Z}) \neq 0$ mit Ordnung 2.

(b) FALSCH. Es sei z.B. $K := \overline{\mathbb{Q}} := \{a \in \mathbb{C} \ : \ a \text{ algebraisch über } \mathbb{Q}\} \supset \mathbb{Q}$ der algebraische Abschluss von $k := \mathbb{Q}$. Da es in $\mathbb{Q}[X]$ irreduzible Polynome beliebigen Grades gibt (z.B. $X^n - 2$), folgt $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

(c) FALSCH. $\mathbb{F}_4$ ist ein Körper (4 ist Primzahlpotenz), also nullteilerfrei. Für $\mathbb{Z}/4\mathbb{Z}$ gilt dies nicht (dort ist $2 \cdot 2 = 4 = 0$). Somit gibt es keinen Ringisomorphismus zwischen den beiden Ringen. (Nullteilerfreiheit bleibt unter Isomorphismen erhalten: Sei $\psi : R_1 \to R_2$ ein Ringisomorphismus und R_2 nullteilerfrei, so ist für $a, b \in R_1$ mit $ab = 0$ auch $0 = \varphi(0) = \varphi(a)\varphi(b)$, also $\varphi(a) = 0$ oder $\varphi(b) = 0$; damit ist wegen der Bijektion $a = 0$ oder $b = 0$.)

Alternativ: $\mathbb{F}_4 = \mathbb{F}_2(\alpha) \cong \mathbb{F}_2[X]/(X^2+X+1)$, wobei α eine Nullstelle von X^2+X+1 sei (laut STRUKTURSATZ FÜR ENDLICHE KÖRPER und direkter Nachweis der Irreduzibilität). Damit ist $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$, und man rechnet in $\mathbb{F}_2(\alpha)$ nach, dass $\mathrm{ord}(1) = \mathrm{ord}(\alpha) = \mathrm{ord}(\alpha+1) = 2$. Somit ist die additive Gruppe von $\mathbb{F}_4$ isomorph zur Kleinschen Vierergruppe, also nicht zu Z_4. Somit gibt es diesen Ringisomorphismus nicht (die additiven Gruppen müssten isomorph sein).

(d) WAHR. Es ist $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$ (mit nach EISENSTEIN irreduziblen Polynom $X^3 - 5$). Mit Zirkel und Lineal wäre $\sqrt[3]{5}$ aber nur dann konstruierbar (laut Ergänzungen), wenn $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}]$ eine Potenz von 2 wäre.

(e) FALSCH. Es gibt laut STRUKTURSATZ FÜR ENDLICHE KÖRPER nur Körper, die p^n Elemente beinhalten, dabei ist p eine Primzahl und $n \in \mathbb{N}$ (jeder endliche Körper beinhaltet ja einen Primkörper $\mathbb{F}_p$ laut Vorlesung). Die Zahl 6 ist jedoch keine Primzahlpotenz.

Aufgabe 2 (11 Punkte) | I | II | **Seite 1**

Es sei $f := (X^2-2)(X^2-11) \in \mathbb{Q}[X]$.

(a) Ermitteln Sie $[\mathbb{Q}(\sqrt{2}, \sqrt{11}) : \mathbb{Q}]$.
(Ohne Beweis verwendbar: $\sqrt{11} \notin \mathbb{Q}(\sqrt{2})$ und $\sqrt{2} \notin \mathbb{Q}(\sqrt{11})$.)

(b) Begründen Sie, dass die Erweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{11}) \supset \mathbb{Q}$ galoissch ist.

(c) Zeigen Sie, dass die Galoisgruppe $\mathrm{Gal}(f; \mathbb{Q})$ aus genau 4 Elementen besteht.

(d) Zeigen oder widerlegen Sie: Es gibt ein $\varphi \in \mathrm{Gal}(f; \mathbb{Q})$ mit $\varphi(\sqrt{2}) = \sqrt{11}$.

(e) Man kann zeigen (Nachweis nicht erforderlich!), dass es in $\mathrm{Gal}(f; \mathbb{Q})$ kein Element der Ordnung 4 gibt. Bestimmen Sie eine Gruppe, die zu $\mathrm{Gal}(f; \mathbb{Q})$ isomorph ist, und begründen Sie Ihre Entscheidung.

(f) Zeigen Sie ohne Rückgriff auf Resultate aus Übungsaufgaben, dass $\mathbb{Q}(\sqrt{2}+\sqrt{11})$ Zerfällungskörper von f über $\mathbb{Q}$ ist.

Lösung:

(a) Für $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{11})$ ist nach GRADFORMEL:

$$[\mathbb{Q}(\sqrt{2}, \sqrt{11}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4,$$

da $X^2 - 2$ nach EISENSTEIN Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$ ist, und $X^2 - 11 \in \mathbb{Q}(\sqrt{2})[X]$ Minimalpolynom von $\sqrt{11}$ über $\mathbb{Q}(\sqrt{2})$ ist (wäre $X^2 - 11 \in \mathbb{Q}(\sqrt{2})[X]$ reduzibel, so wäre $[\mathbb{Q}(\sqrt{2}, \sqrt{11}) : \mathbb{Q}(\sqrt{2})] = 1$ also $\mathbb{Q}(\sqrt{2}, \sqrt{11}) = \mathbb{Q}(\sqrt{2})$, was aber wegen $\sqrt{11} \notin \mathbb{Q}(\sqrt{2})$ nicht gelten kann).

(b) Nullstellen von f sind $\pm\sqrt{2}$ und $\pm\sqrt{11}$. Somit ist $\mathbb{Q}(\pm\sqrt{2}, \pm\sqrt{11}) = \mathbb{Q}(\sqrt{2}, \sqrt{11})$ Zerfällungskörper, und damit nach Definition galoissch.

(c) Die Ordnung der Galoisgruppe ergibt sich als $[K : \mathbb{Q}]$, wobei K der Zerfällungskörper von f über $\mathbb{Q}$ ist. Den haben wir in (b) schon bestimmt. Somit ergibt sich mit (a):

$$\mathrm{ord}(\mathrm{Gal}(f; \mathbb{Q})) = [\mathbb{Q}(\sqrt{2}, \sqrt{11}) : \mathbb{Q}] = 4.$$

(d) Ein solches φ gibt es nicht, denn sonst wäre

$$2 = \varphi(2) = \varphi(\sqrt{2} \cdot \sqrt{2}) = \varphi(\sqrt{2})\varphi(\sqrt{2}) = \sqrt{11} \cdot \sqrt{11} = 11,$$

was in $\mathbb{Q}$ bekanntlich nicht gilt.

(e) Es gibt nur zwei Gruppen der Ordnung 4: Die Z_4 und die Kleinsche Vierergruppe. Die Z_4 ist zyklisch (d.h. es gibt ein Element der Ordnung 4). Somit muss es sich bei $\mathrm{Gal}(f; \mathbb{Q})$ um die Kleinsche Vierergruppe handeln.

(f) Es ist $\sqrt{2} + \sqrt{11} \in \mathbb{Q}(\sqrt{2}, \sqrt{11})$, also $\mathbb{Q}(\sqrt{2} + \sqrt{11}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{11})$. Andererseits ist

$$\underbrace{(\sqrt{2} + \sqrt{11})}_{\in \mathbb{Q}(\sqrt{2}+\sqrt{11})}(\sqrt{2} - \sqrt{11}) = \underbrace{-9}_{\in \mathbb{Q}(\sqrt{2}+\sqrt{11})} \quad \Rightarrow \quad \sqrt{2} - \sqrt{11} = -9(\sqrt{2} + \sqrt{11})^{-1}$$

also $\sqrt{2} - \sqrt{11} \in \mathbb{Q}(\sqrt{2} + \sqrt{11})$. Damit ist aber

$$\begin{aligned} \sqrt{2} &= \frac{1}{2}(\sqrt{2} + \sqrt{11}) + \frac{1}{2}(\sqrt{2} - \sqrt{11}) \in \mathbb{Q}(\sqrt{2}, \sqrt{11}), \\ \sqrt{11} &= \frac{1}{2}(\sqrt{2} + \sqrt{11}) - \frac{1}{2}(\sqrt{2} - \sqrt{11}) \in \mathbb{Q}(\sqrt{2}, \sqrt{11}), \end{aligned}$$

also $\mathbb{Q}(\sqrt{2}, \sqrt{11}) \subset \mathbb{Q}(\sqrt{2} + \sqrt{11})$.

Aufgabe 3 (6 Punkte)

I	II

Seite 2

(a) Geben Sie drei nicht-isomorphe Gruppen der Ordnung 2016 an (mit Begründung).

(b) Die Gruppe $G := \mathbb{Z}/2016\mathbb{Z}$ hat eine zyklische Untergruppe mit 1008 Elementen. Zeigen Sie, dass diese Untergruppe ein Normalteiler von G ist.

Lösung:

(a) Wir haben die Primzahlzerlegung $2016 = 2^5 \cdot 3^2 \cdot 7$. Laut Struktursatz für endliche abelsche Gruppen haben wir einen verschiedenen Isomorphietyp für jede unterschiedliche Zerlegung der 2016 in Primzahlpotenzen. Beispielsweise haben wir folgende drei unterschiedliche endliche abelsche Gruppen der Ordnung 2016:

$$Z_{2^5} \times Z_{3^2} \times Z_7, \qquad Z_2 \times Z_{2^4} \times Z_{3^2} \times Z_7, \qquad Z_2 \times Z_2 \times Z_{2^3} \times Z_{3^2} \times Z_7.$$

(b) Sei Z_{1008} die entsprechende zyklische Untergruppe von $G = Z_{2016}$. Dann ist der Index von Z_{1008} in Z_{2016}:

$$\mathrm{ind}(Z_{2016} : Z_{1008}) = \mathrm{ord}(Z_{2016}) : \mathrm{ord}(Z_{1008}) = 2016 : 1008 = 2.$$

Jede Untergruppe mit Index 2 ist jedoch ein Normalteiler in Z_{2016} (das haben wir in einer Übungsaufgabe gezeigt). Somit ist die Aussage gezeigt.

Aufgabe 4 (7 Punkte) | I | II | **Seite 2**

(a) Zeigen Sie, dass $g := X^2 - X - 1 \in \mathbb{Q}[X]$ über $\mathbb{Q}$ irreduzibel ist.

(b) Bestimmen Sie die Galoisgruppe $\mathrm{Gal}(g; \mathbb{Q}(\sqrt{5}))$ von g über $\mathbb{Q}(\sqrt{5})$.

Lösung:

(a) Wäre g reduzibel, so hätte g eine Nullstelle in $\mathbb{Q}$. Die Nullstellen von g sind jedoch $\frac{1}{2} + \frac{1}{2}\sqrt{5}$ und $\frac{1}{2} - \frac{1}{2}\sqrt{5}$ (Mitternachtsformel). Wegen $\sqrt{5} \notin \mathbb{Q}$ liegen diese nicht in $\mathbb{Q}$. Somit ist g irreduzibel über $\mathbb{Q}$.

(b) Die beiden Nullstellen von $g \in \mathbb{Q}(\sqrt{5})[X]$ liegen offensichtlich in $\mathbb{Q}(\sqrt{5})$. Somit ist $\mathbb{Q}(\sqrt{5})$ auch Zerfällungskörper von g über $\mathbb{Q}(\sqrt{5})$. Jetzt ist

$$\mathrm{ord}(\mathrm{Gal}(g; \mathbb{Q}(\sqrt{5}))) = [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}(\sqrt{5})] = 1.$$

Somit ist $\mathrm{Gal}(g; \mathbb{Q}(\sqrt{5})) = \{\mathrm{id}\}$.

Aufgabe 5 (6 Punkte) | I | II | **Seite 3**

(a) Zeigen Sie, dass $h := X^4 + X^3 + 1 \in \mathbb{F}_2[X]$ irreduzibel über $\mathbb{F}_2$ ist.

(b) Zeigen Sie, dass $K := \mathbb{F}_2[X]/(h)$ ein Körper mit 16 Elementen ist, und geben Sie (bis auf Isomorphie) alle Zwischenkörper $\mathbb{F}_2 \subset L \subset K$ an.

Lösung:

(a) Wäre h reduzibel, so hätte h entweder eine Nullstelle in $\mathbb{F}_2$ oder zwei irreduzible quadratische (und o.B.d.A. normierte) Teiler. Es gibt keine Nullstellen da

$$h(0) = 1 \neq 0, \qquad h(1) = 1 \neq 0.$$

Es bleibt der Fall zweier normierter quadratischer Teiler:

$$\begin{aligned} h &= (X^2 + \lambda_1 X + \lambda_0)(X^2 + \mu_1 X + \mu_0) \\ &= X^4 + \underbrace{(\lambda_1 + \mu_1)}_{=1} X^3 + \underbrace{(\lambda_0 + \mu_0 + \lambda_1\mu_1)}_{=0} X^2 + \underbrace{(\lambda_1\mu_0 + \lambda_0\mu_1)}_{=0} X + \underbrace{\lambda_0\mu_0}_{=1} \end{aligned}$$

für $\lambda_0, \lambda_1, \mu_1, \mu_2 \in \mathbb{F}_2$. Für den Koeffizienten von X^3 haben wir (o.B.d.A) $\lambda_1 = 1$, $\mu_1 = 0$. Für den Koeffizienten von X^0 haben wir $\lambda_0\mu_0 = 1$, was in $\mathbb{F}_2$ äquivalent zu $\lambda_0 = \mu_0 = 1$ ist. Setzen wir in $\lambda_1\mu_0 + \lambda_0\mu_1 = 0$ ein, so erhalten wir $1 = 0$, was in $\mathbb{F}_2$ nicht gilt.

Somit ist h irreduzibel.

(b) Laut Strukturssatz über endliche Körper und (a) ist $\mathbb{F}_2[X]/(h) \cong \mathbb{F}_{2^{\deg(h)}} = \mathbb{F}_{16}$. Laut Strukturssatz über endliche Körper haben wir die Zwischenkörper

$$\mathbb{F}_2 \subset \mathbb{F}_{2^2} \subset \mathbb{F}_{2^4}.$$