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) Der Körper $\mathbb{F}_9$ ist ein Unterkörper von $\mathbb{F}_{27}$.

(b) Es gilt $[\mathbb{R} : \mathbb{Q}] = \infty$.

(c) Es gibt einen Körperautomorphismus $\varphi : \mathbb{Q}(i) \to \mathbb{Q}(i)$ mit $\varphi(i) = 2i$.

(d) Sind $K \supseteq L \supseteq k$ Körpererweiterungen und ist $K \supseteq k$ galoissch, so ist auch $L \supseteq k$ galoissch.

(e) Die Primrestklassengruppe $Z_8^\times$ ist zyklisch.

Lösung:

(a) FALSCH. Laut STRUKTURSATZ FÜR ENDLICHE KÖRPER sind die Unterkörper von $\mathbb{F}_{3^3}$ genau die Körper $\mathbb{F}_3$ und $\mathbb{F}_{3^3}$ (Exponent teilt die 3).

(b) RICHTIG. Für jedes $n \in \mathbb{N}$ ist $X^n - 2$ irreduzibel (EISENSTEIN). Für $\sqrt[n]{2} \in \mathbb{R}_+$ ist somit $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[n]{2}) \subseteq \mathbb{R}$, also $[\mathbb{R} : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$.

(c) FALSCH. Ansonsten erhält man den Widerspruch:

$$-1 = -\varphi(1) = \varphi(-1) = \varphi(i \cdot i) = \varphi(i) \cdot \varphi(i) = 2i \cdot 2i = -4.$$

(d) FALSCH. Gegenbeispiel aus der Vorlesung: $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.

(e) FALSCH. Die $Z_8^\times$ besteht aus den zu 8 teilerfremden Klassen $\overline{1}, \overline{3}, \overline{5}, \overline{7}$. Die Klassen $\overline{3}, \overline{5}, \overline{7}$ haben Ordnung 2. Somit handelt es sich hier um die Kleinsche Vierergruppe und nicht um Z_4.

Aufgabe 2 (4 Punkte) | I | II | **Seite 1**

Es sei $\alpha \in \mathbb{C}$ Nullstelle des Polynoms

$$f := X^2 + 2X + 2 \in \mathbb{Q}[X].$$

(a) Zeigen Sie, dass $(1, \alpha)$ eine Basis von $\mathbb{Q}(\alpha)$ über $\mathbb{Q}$ ist.

(b) Schreiben Sie $(\alpha + 2)^{-1}$ als Linearkombination bezüglich der Basis $(1, \alpha)$.

Lösung:

(a) Das Polynom f ist irreduzibel nach EISENSTEIN. Somit ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ und $(1, \alpha)$ eine Basis von $\mathbb{Q}(\alpha)$ über $\mathbb{Q}$.

(b) Es gilt:

$$\alpha(\alpha + 2) + 2 = 0 \qquad \Leftrightarrow \qquad 1 = -\frac{1}{2}\alpha(\alpha + 2),$$

also $(\alpha + 2)^{-1} = -\frac{1}{2}\alpha$.

Alternativ: Durch Koeffizientenvergleich ermitteln wir die Koeffizienten $\lambda_0, \lambda_1 \in \mathbb{Q}$ von $(\alpha+2)^{-1} = \lambda_0 + \lambda_1\alpha$: Aus $(\alpha + 2)(\lambda_0 + \lambda_1\alpha) = 1$ erhalten wir $\lambda_0\alpha + 2\lambda_0 - 2\lambda_1 = 1$, also $\lambda_0 = 0$ und $\lambda_1 = -\frac{1}{2}$.

Aufgabe 3 (11 Punkte) | I | II | **Seite 2**

Zeigen Sie:

(a) $f := X^2 + X + 1 \in \mathbb{Q}(\pi)[X]$ ist irreduzibel.

(b) Der Zerfällungskörper von $g := X^3 - \pi \in \mathbb{Q}(\pi)[X]$ ist $L := \mathbb{Q}(\pi, \sqrt[3]{\pi}, \xi)$, wobei $\xi := \exp(2\pi i/3)$.

(c) Es gilt $[\mathbb{Q}(\pi, \sqrt[3]{\pi}) : \mathbb{Q}(\pi)] = 3$. (Sie dürfen ohne Beweis $\sqrt[3]{\pi} \notin \mathbb{Q}(\pi)$ verwenden.)

(d) Die Körpererweiterung $L \supseteq \mathbb{Q}(\pi)$ ist galoissch.

(e) Die Galoissgruppe $\mathrm{Gal}(g; \mathbb{Q}(\pi))$ besteht aus 6 Elementen.

Lösung:

(a) Das Polynom f hat die Nullstellen $\xi := \exp(2\pi i/3) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ und $\xi^2 = \exp(4\pi i/3) = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$. Diese liegen nicht in $\mathbb{Q}(\pi) \subseteq \mathbb{R}$, somit ist f irreduzibel über $\mathbb{Q}(\pi)$.

(b) Das Polynom g hat die Nullstellen $\sqrt[3]{\pi}$, $\sqrt[3]{\pi}\xi$ und $\sqrt[3]{\pi}\xi^2$. Somit ist $\mathbb{Q}(\sqrt[3]{\pi}, \sqrt[3]{\pi}\xi, \sqrt[3]{\pi}\xi^2)$ Zerfällungskörper von g. Offensichtlich ist

$$\mathbb{Q}(\sqrt[3]{\pi}, \sqrt[3]{\pi}\xi, \sqrt[3]{\pi}\xi^2) = \mathbb{Q}(\pi, \sqrt[3]{\pi}, \xi) = L.$$

(c) Das Polynom g hat keine Nullstellen in $\mathbb{Q}(\pi) \subseteq \mathbb{R}$ (wegen $\sqrt[3]{\pi} \notin \mathbb{Q}(\pi)$ und $\sqrt[3]{\pi}\xi, \sqrt[3]{\pi}\xi^2 \in \mathbb{C} \setminus \mathbb{R}$). Somit ist g Minimalpolynom von $\sqrt[3]{\pi}$ über $\mathbb{Q}(\pi)$. Damit ist

$$[\mathbb{Q}(\pi, \sqrt[3]{\pi}) : \mathbb{Q}(\pi)] = \deg(g) = 3.$$

(d) Die Körpererweiterung L ist nach (b) Zerfällungskörper des Polynoms $g \in \mathbb{Q}(\pi)[X]$, also galoissch.

(e) Da L nach (b) Zerfällungskörper von $g \in \mathbb{Q}(\pi)[X]$ ist, ist laut Theorem zur Charakterisierung von Galois-Erweiterungen

$$\mathrm{ord}(\mathrm{Gal}(g; \mathbb{Q}(\pi))) = [L : \mathbb{Q}(\pi)].$$

Laut Gradformel gilt:

$$[L : \mathbb{Q}(\pi)] = [\mathbb{Q}(\pi, \sqrt[3]{\pi}, \xi) : \mathbb{Q}(\pi)] = \underbrace{[\mathbb{Q}(\pi, \sqrt[3]{\pi}, \xi) : \mathbb{Q}(\pi, \sqrt[3]{\pi})]}_{=\deg(f)=2 \text{ nach (a)}} \cdot \underbrace{[\mathbb{Q}(\pi, \sqrt[3]{\pi}) : \mathbb{Q}(\pi)]}_{=3 \text{ nach (c)}} = 6.$$

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

Es sei $R := \mathbb{Z}[i\sqrt{2}] = \{a + bi\sqrt{2} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ gegeben. Sie dürfen ohne Beweis verwenden, dass R bezüglich der Normfunktion

$$N : R \to \mathbb{N}, \qquad a + bi\sqrt{2} \mapsto a^2 + 2b^2$$

ein euklidischer Ring ist.

(a) Bestimmen Sie die Einheiten von R.

(b) Bestimmen und begründen Sie, welche der Zahlen 2 und 7 Primelemente in R sind.

Lösung:

(a) Die Elemente ± 1 sind Einheiten, da

$$1 \cdot 1 = 1, \qquad (-1) \cdot (-1) = 1.$$

Es gibt keine weiteren Einheiten, denn jede Einheit $z = a + bi\sqrt{2}$ erfüllt $1 = N(1) = N(z \cdot z^{-1}) = N(z) \cdot N(z^{-1})$, was wegen $N(R) \subseteq \mathbb{N}$ bedeutet, dass $1 = N(z) = a^2 + 2b^2$, also $b = 0$ und $a = \pm 1$ gelten muß. Somit ist die Einheitengruppe $R^\times = \{\pm 1\}$.

(b)
- Die Zahl 2 ist nicht prim, da
$$2 = (i\sqrt{2}) \cdot (-i\sqrt{2})$$
mit Nicht-Einheiten $\pm i\sqrt{2}$.
- Die Zahl 7 ist Primzahl, denn wäre 7 zerlegbar, also $7 = x \cdot y$ mit $x, y \in R \setminus R^\times$, so folgt
$$49 = N(7) = N(x)N(y) \qquad \Rightarrow N(x) = N(y).$$
In R gibt es allerdings keine Elemente mit $N(x) = 7$, wie man leicht aus der Ganzzahligkeit der Koeffizienten a, b von $x = a + bi\sqrt{2}$ aus $7 = N(x) = a^2 + 2b^2$ folgern kann (betrachte die Fälle, $a \in \{\pm 2, \pm 1, 0\}, b \in \{\pm 1, 0\}$).

Aufgabe 5 (8 Punkte) | I | II | **Seite 3**

Es sei $(G, \cdot)$ eine endliche Gruppe, $a \in G$ und $\varphi : \mathbb{Z} \to G$ mit $\varphi(n) = a^n$.

(a) Zeigen Sie, dass φ ein Homomorphismus ist.

(b) Zeigen Sie, dass φ auf $\mathrm{Erz}(a)$ surjektiv abbildet.

(c) Bestimmen Sie den Kern von φ.

(d) Zeigen Sie, dass eine natürliche Zahl $m > 0$ existiert mit $\mathrm{Erz}(a) \cong \mathbb{Z}/m\mathbb{Z}$.

Lösung:

(a) Für $k, l \in \mathbb{Z}$ gilt
$$\varphi(k+l) = a^{k+l} = \underbrace{a \cdot \ldots \cdot a}_{k+l \text{ mal}} = a^k a^l = \varphi(k)\varphi(l).$$

(b) Es sei $x \in \mathrm{Erz}(a)$, also $x = a^n$ für ein $n \in \mathbb{N}$. Natürlich ist dann $x = \varphi(n)$, also $\varphi : \mathbb{Z} \to \mathrm{Erz}(a)$ surjektiv.

(c) $\mathrm{Ker}\,\varphi$ ist laut Vorlesung eine Untergruppe von $\mathbb{Z}$. Diese sind immer von der Form $m\mathbb{Z}$ mit einem $m \in \mathbb{N}$. In unserem Fall ist $m \neq 0$, da φ die unendliche Menge $\mathbb{Z}$ nicht injektiv auf die endliche Gruppe G abbilden kann.

(d) Der ERSTE ISOMORPHIESATZ besagt (da $\varphi : \mathbb{Z} \to \mathrm{Erz}(a)$ surjektiv nach (b)), dass
$$\mathrm{Erz}(a) \cong \mathbb{Z}/\mathrm{Ker}\,\varphi$$
gilt, was nach (c) auf
$$\mathrm{Erz}(a) \cong \mathbb{Z}/m\mathbb{Z},$$
mit $m > 0$ hinausläuft.
