

9. Übung zur Algebra 1

9.1. (Adjunktion) (4 Punkte)

- (a) Zeigen Sie, dass $\mathbb{Q}[\sqrt{2}]$, der kleinste Teilring von $\mathbb{C}$, welcher $\mathbb{Q} \cup \{\sqrt{2}\}$ enthält, sogar ein Körper ist.
- (b) Es sei $\alpha \in \mathbb{C}$ eine komplexe Zahl, welche Nullstelle keines nicht-konstanten Polynoms mit rationalen Koeffizienten ist (d.h. für alle $n \in \mathbb{N}_0$ und alle $a_0, a_1, \dots, a_n \in \mathbb{Q}$ mit $\{a_0, a_1, \dots, a_n\} \neq \{0\}$ ist $a_0 + a_1\alpha + \dots + a_n\alpha^n \neq 0$). Zeigen Sie, dass $\mathbb{Q}[\alpha]$ kein Körper ist.

9.2. (Endliche Integritätsbereiche sind Körper) (4 Punkte)

R sei ein **Integritätsbereich**, d.h. ein kommutativer Ring ungleich dem Nullring, sodass für alle $a, b \in R$ aus $ab = 0_R$ schon $a = 0_R$ oder $b = 0_R$ folgt.

- (a) Zeigen Sie, dass für alle $a \in R \setminus \{0_R\}$ die Abbildung $R \rightarrow R$, $b \mapsto ab$, injektiv ist.
- (b) Folgern Sie: ist $\#R < \infty$, so ist R ein Körper.

9.3. (Einheitengruppe von $\mathbb{Z}/2^v\mathbb{Z}$) (4 Punkte)

Es sei $v \in \mathbb{N} \setminus \{1, 2\}$ und $(\mathbb{Z}/2^v\mathbb{Z})^\times$ bezeichne die Einheitengruppe des Rings $\mathbb{Z}/2^v\mathbb{Z}$. Beweisen Sie die folgenden Aussagen:

- (a) Es gibt ein $m \in \mathbb{N}$ mit $5^{2^{v-2}} = 1 + m2^v$. (Hinweis: Induktion über v .)
- (b) Für $v \geq 2$ liegt $5 \bmod 2^v$ in $(\mathbb{Z}/2^v\mathbb{Z})^\times$ und hat die Ordnung 2^{v-2} .
- (c) Für $v \geq 2$ ist $(\mathbb{Z}/2^v\mathbb{Z})^\times \cong C_2 \times C_{2^{v-2}}$.
(Hinweis: finden Sie zunächst zwei verschiedene Elemente von $(\mathbb{Z}/2^v\mathbb{Z})^\times$ mit Ordnung 2. Überlegen Sie sich dann, welche Möglichkeiten für $q_1, \dots, q_t$ in Satz 5.3 im vorliegenden Fall in Frage kommen.)

9.4. (Normen) (4 Punkte)

Es sei $d \neq 1$ eine **quadratfreie** ganze Zahl, d.h. es gibt kein $n \in \mathbb{N} \setminus \{1\}$ mit $n^2 \mid d$. Mit $\sqrt{d}$ sei eine beliebige komplexe Nullstelle des Polynoms $X^2 - d$ bezeichnet. (Die zweite solche Nullstelle ist dann $-\sqrt{d}$.) Es sei $\vartheta = \sqrt{d}$ falls $d \equiv 2, 3 \bmod 4$ und $\vartheta = \frac{1}{2}(1 + \sqrt{d})$ falls $d \equiv 1 \bmod 4$. (Der Fall $d \equiv 0 \bmod 4$ kann wegen Quadratfreiheit von d nicht eintreten.) $\mathbb{Z}[\vartheta]$ bezeichne den kleinsten Teilring von $\mathbb{C}$, der $\mathbb{Z}$ und ϑ enthält. $\mathbb{Q}[\vartheta]$ sei analog definiert.

- (a) Zeigen Sie $\vartheta \notin \mathbb{Q}$, $\mathbb{Z}[\vartheta] = \{a + b\vartheta \in \mathbb{C} : a, b \in \mathbb{Z}\}$ und $\mathbb{Q}[\vartheta] = \{a + b\vartheta \in \mathbb{C} : a, b \in \mathbb{Q}\}$.

- (b) Bestimmen Sie für $a, b \in \mathbb{Z}$ die Darstellungsmatrix $A_{a+b\vartheta}$ der $\mathbb{Q}$ -linearen Abbildung $\mathbb{Q}[\vartheta] \rightarrow \mathbb{Q}[\vartheta]$, $x \mapsto (a + b\vartheta)x$, bezüglich der $\mathbb{Q}$ -Basis $1, \vartheta$ von $\mathbb{Q}[\vartheta]$.
- (c) Zeigen Sie, dass $\det(A_{a+b\vartheta})$ für $a, b \in \mathbb{Z}$ eine ganze Zahl ist und die Abbildung $N: \mathbb{Z}[\vartheta] \rightarrow \mathbb{Z}$, $y \mapsto \det(A_y)$, multiplikativ ist (d.h. $N(xy) = N(x)N(y)$ für alle $x, y \in \mathbb{Z}[\vartheta]$).
- (d) Zeigen Sie: $x \in (\mathbb{Z}[\vartheta])^\times \iff N(x) \in \mathbb{Z}^\times = \{\pm 1\}$.