22. November 2017

Algebra und Zahlentheorie [1]
Übungsblatt 6

Aufgabe 6.1. Sei $\mathbb{C}$ der Körper der komplexen Zahlen. Zur Erinnerung: $\mathbb{C}$ is ein zwei dimensionaler $\mathbb{R}$-Vektorraum mit Basis $1, i$ und die Multiplikation zweier Elemente $z = x + iy$ und $z' = x' + iy'$, $x, x', y, y' \in \mathbb{R}$, ist folgendermaßen definiert

$$zz' = (xx' - yy') + i(xy' + x'y).$$

Wir definieren die Teilmenge der Gaußschen Zahlen wie folgt:

$$\mathbb{Z}[i] := \{a + ib \mid a, b \in \mathbb{Z}\}.$$

(1) Zeigen Sie, dass $\mathbb{Z}[i] \subset \mathbb{C}$ ein Unterring ist (d.h. er ist eine (additive) Untergruppe, enthält die 1 und ist abgeschlossen bzgl. der Multiplikation).
(2) Zeigen Sie, dass $\mathbb{Z}[i]$ integer ist.
(3) Zeigen Sie, dass

$$\mathbb{Z}[i] \to \mathbb{Z}[i], \quad \alpha = a + ib \mapsto \bar{\alpha} := a - ib$$

ein Ringisomorphismus ist.
(4) Zeigen Sie, dass $\mathbb{Z}[i]$ ein euklidischer Ring ist bzgl. der Abbildung $\mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}$, $\alpha \mapsto |\alpha|^2 := \alpha\bar{\alpha}$, d.h. zeigen Sie, für alle $\alpha, \beta \in \mathbb{Z}[i]$, existieren $\gamma, \rho \in \mathbb{Z}[i]$ mit

$$\alpha = \gamma\beta + \rho \text{ und } |\rho|^2 < |\beta|^2.$$

(*Hinweis:* Beachten Sie zuerst, für jede rationale Zahl $q \in \mathbb{Q}$ gibt es eine ganze Zahl $m \in \mathbb{Z}$ mit $(q - m)^2 \leq \frac{1}{4}$. Zeigen Sie nun, es gibt ein $\gamma \in \mathbb{Z}[i]$ mit $|\frac{\alpha}{\beta} - \gamma|^2 < 1$ und schließen Sie.)
(5) Ist $2 = 2 + i \cdot 0 \in \mathbb{Z}[i]$ ein Primelement?

Aufgabe 6.2. Sei $\mathbb{Z}[X]$ der Polynomring in einer Variablen mit Koeffizienten in $\mathbb{Z}$. Zeigen Sie, dass $\mathbb{Z}[X]$ kein Hauptidealring ist (und somit auch nicht euklidisch).

Aufgabe 6.3. Sei $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ der Körper mit zwei Elementen.

(1) Zeigen Sie, dass $\mathbb{F}_4 := \mathbb{F}_2[X]/(X^2 + X + 1)$ ein Körper mit 4 Elementen ist.
(2) Aus der Vorlesung wissen wir, dass 1, $\alpha := \bar{X}$ eine Basis von $\mathbb{F}_4$ als $\mathbb{F}_2$-Vektorraum ist. Schreiben Sie die Restklasse von $X^5 + 7X^4 + 4X^3 + 2X^2 + X + 1$ in $\mathbb{F}_4$ in dieser Basis. (*Hinweis:* Polynomdivision.)

[1] Fragen oder Kommentare an `kay.ruelling@fu-berlin.de` oder `filip@zedat.fu-berlin.de`

Aufgabe 6.4. Sei $\mathbb{R}$ der Körper der reellen Zahlen. Zeigen Sie, es gibt einen Isomorphismus von Ringen

$$\mathbb{R}[X]/(X^4 - 1) \xrightarrow{\simeq} \mathbb{R} \times \mathbb{R} \times \mathbb{C}, \quad \bar{f} \mapsto (f(1), f(-1), f(i)).$$

(*Hinweis:* Chinesischer Restklassensatz und Aufgabe 4.4(4).)