CARL VON OSSIETZKY universität OLDENBURG

Algebra - SS 20
Prof. Dr. Anne Frühbis-Krüger
M.Sc. Marco Melles

Präsenzaufgaben 4

Keine Abgabe vorgesehen

Präsenzaufgabe 4.5 (Erweiterter Euklidischer Algorithmus)**.** Es sei R ein euklidischer Ring mit zugehöriger Abbildung $d : R \setminus \{0\} \longrightarrow \mathbb{N}_0$. Für beliebige $a, b \in R$ mit $b \neq 0$ definieren wir $r_{-1} := a$ und $r_0 := b$. Es seien $(r_j)_{j=1}^{n}$ und $(q_j)_{j=0}^{n-1}$ die in Bemerkung 2.7.10. eindeutig definierten Folgen des euklidischen Algorithmus:

$$r_{j+1} := r_{j-1} - q_j\, r_j, \qquad \text{wobei } d(r_{j+1}) < d(r_j) \text{ oder } r_{j+1} = 0.$$

Hierbei sei n die kleinste natürliche Zahl, sodass $r_n = 0$. Wir definieren weiter die Folgen $(x_j)_{j=-1}^{n-1}$ und $(y_j)_{j=-1}^{n-1}$ mittels

$$\begin{aligned} x_{-1} &:= 1, \quad x_0 := 0, \quad x_{j+1} := x_{j-1} - q_j x_j \quad \text{für } j \in \{0\,, \ldots\,, n-1\} \\ y_{-1} &:= 0, \quad y_0 := 1, \quad y_{j+1} := y_{j-1} - q_j y_j \quad \text{für } j \in \{0\,, \ldots\,, n-1\}. \end{aligned}$$

(**a**). Führen Sie den erweiterten euklidischen Algorithmus am Beispiel $a = 86$ und $b = 24$ aus.

(**b**). Zeigen Sie, dass $r_j = x_j\, a \,+\, y_j\, b$ für alle $j \in \{-1, \ldots, n-1\}$. Vergewissern Sie sich, dass damit die Korrektheit des Algorithmus bewiesen ist und wir eine Bézout-Darstellung eines größten gemeinsamen Teilers von a und b erhalten mittels

$$r_{n-1} \;=\; x_{n-1}\, a \,+\, y_{n-1}\, b.$$

(**c**). Formulieren Sie diesen Algorithmus analog zum euklidischen Algorithmus aus der Vorlesung als WHILE-Schleife zur Bestimmung einer Bézout-Darstellung eines größten gemeinsamen Teilers von a und b.

Präsenzaufgabe 4.6. Berechnen Sie jeweils mittels des erweiterten euklidischen Algorithmus eine Bézout-Darstellung eines größten gemeinsamen Teilers von $a \in R$ und $b \in R$ für

(**a**). $R = \mathbb{Z}$, $a = 217$ und $b = 133$.

(**b**). $R = \mathbb{Q}[t]$, $a = t^4 + 14t^3 + 59t^2 + 46t - 120$ und $b = t^3 + 4t^2 + t - 6$.

Präsenzaufgabe 4.7. Für quadratfreies $d \in \mathbb{N} \setminus \{1\}$, d.h. in der Primfaktorzerlegung von d tauchen die Primzahlen höchstens mit Vielfachheit 1 auf, sei $\mathbb{Z}[\sqrt{d}\,] = \{\, a + b\sqrt{d} \mid a\,, b \in \mathbb{Z}\,\}$, ein Unterring von $\mathbb{R}$. Wir definieren

$$\begin{aligned} N \,:\, \mathbb{Z}[\sqrt{d}\,] &\longrightarrow \mathbb{Z} \\ a + b\sqrt{d} &\longmapsto N(\,a + b\sqrt{d}\,) \,=\, a^2 - d\,b^2\,. \end{aligned}$$

(**a**). Beweisen Sie die folgenden Aussagen.

(a) Für alle $\alpha\,, \beta \in \mathbb{Z}[\sqrt{d}\,]$ gilt: $N(\,\alpha\,\beta\,) = N(\,\alpha\,)\,N(\,\beta\,)$. Insbesondere: $N(\,\alpha\,) = 0 \Leftrightarrow \alpha = 0$.

(b) $N(\,\alpha\,) = \pm 1 \Leftrightarrow \alpha \in \mathbb{Z}[\sqrt{d}\,]^*$. Ermitteln Sie damit 4 Elemente von $\mathbb{Z}[\sqrt{10}\,]^*$.

(**b**). $2\,, 3\,, 4 + \sqrt{10}\,, 4 - \sqrt{10}$ sind irreduzible Elemente, jedoch keine Primelemente von $\mathbb{Z}[\sqrt{10}\,]$.
Hinweis: $2 \cdot 3 = (4 + \sqrt{10})\,(4 - \sqrt{10}\,)$ *und rechnen Sie ggfs. in* $\mathbb{Z}/10\mathbb{Z}$ *mittels Reduktion.*