**Dr. Markus Junker — Mathematik II für Informatiker — Sommer 2013**
Übungsblatt 9

---

Verantwortlich für die Übungen:
Dr. Blaž Mramor (blaz.mramor@math.uni-freiburg.de)

1. **Das Zentrum der** $\mathrm{GL}_N$ (4 Punkte). Sei $\mathrm{GL}_N(\mathbb{R})$ die Gruppe der invertierbaren $N \times N$-Matrizen über $\mathbb{R}$. Beweisen Sie:

$$Z(\mathrm{GL}_N(\mathbb{R})) = \left\{ \begin{pmatrix} \lambda & 0 & \dots & 0 \\ 0 & \lambda & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda \end{pmatrix} \middle| \lambda \in \mathbb{R} \backslash \{0\} \right\}.$$

*Hinweis: Untersuchen Sie die Vertauschungsbedingung für die Vertauschung mit geeigneten Elementarmatrizen $E_{i,j}$ explizit, wobei der $(k,l)$-te Eintrag der Matrix $E_{i,j}$ gegeben ist durch*

$$(E_{i,j})_{k,l} = \begin{cases} 1 & \text{wenn} \quad k = i, l = j \\ 0 & \text{sonst.} \end{cases}$$

2. **Der euklidische Algorithmus** (6 Punkte).

Für gegebene $a, b \in \mathbb{N}$ mit $a > b > 0$, suchen wir $\mathrm{ggT}(a,b)$. Dazu definieren wir induktiv $r_n \in \mathbb{N}$ durch $r_0 := a$, $r_1 := b$ und $r_{i-1} = q_i \cdot r_i + r_{i+1}$, wobei $r_{i+1}$ der Rest von $r_i$ bei Division mit $r_{i-1}$ ist.

In jedem Schritt $i$ gilt entweder $r_i = 0$, oder $0 < r_i < r_{i-1}$, also kommt dieser Algorithmus in endlich viele Schritten bei 0 an. Sei $N \in \mathbb{N}$ der größte Index mit $r_N > 0$, also muss gelten $r_N | r_{N-1}$.

(a) Zeigen Sie, dass $\mathrm{ggT}(r_i, r_{i-1}) = \mathrm{ggT}(r_{i-1}, r_{i-2})$ für alle $i \in \mathbb{N}$ mit $i \leq N$ gilt, und dass $r_N = \mathrm{ggT}(a,b)$.

(b) Zeigen Sie, dass wenn man sich die Konstanten $q_i$ und $r_i$ merkt, das Rückwärtz-Ausführen von dem euklidischen Algorithmus eine Darstellung $ggT(a,b) = k \cdot a + l \cdot b$ ergibt mit $k, l \in \mathbb{Z}$.

(c) Beweisen Sie, dass $ggT(a,b)$ definiert werden kann, als die kleinste positive natürliche Zahl $n \in \mathbb{N}$, s.d. es zwei ganze Zahlen $k, l \in \mathbb{Z}$ gibt, mit $n = k \cdot a + l \cdot b$.

(d) Wenden Sie den euklidischen Algorithmus auf die Zahlen 26 und 42 an, und finden Sie eine Darstellung

$$k \cdot 26 + l \cdot 42 = \mathrm{ggT}(26, 42).$$

mit ganzen Zahlen $k$ und $l$. Geben Sie alle Zwischenschritte an.

*Bitte wenden!*

3. **Die Einheitengruppe der Restklassen** (6 Punkten). Wie in Aufgabe 2, Übungsblatt 2, bezeichnen wir mit $\mathbb{Z}/N\mathbb{Z}$ die Restklassen modulo $N$.

Definiere

$$(\mathbb{Z}/N\mathbb{Z})^* := \{\overline{x} \in \mathbb{Z}/N\mathbb{Z} \mid \operatorname{ggT}(x, N) = 1\}.$$

(a) Zeigen Sie, dass dies eine sinnvolle Definition ist, d.h. dass die Bedingung $\operatorname{ggT}(x, N) = 1$ nicht von der Wahl des Vertreters $x$ abhängt.

(b) Beweisen Sie, dass die Menge $(\mathbb{Z}/N\mathbb{Z})^*$ bzgl. der Operation „·“ eine Gruppe bildet.

*Bemerkung: Sie können die Aussagen von Aufgabe 2, Übungsblatt 2 annehmen.*

(c) Bestimmen Sie für die Gruppen $(\mathbb{Z}/5\mathbb{Z})^*$ und $(\mathbb{Z}/8\mathbb{Z})^*$ die Gruppentafel. Welche Ordnung haben diese beiden Gruppen? Welche der beiden Gruppen sind zyklisch?

*Hinweis: Benutzen Sie Aufgabe 2, die zeigt, dass* $\operatorname{ggT}(x, N) = 1$ *genau dann gilt, wenn es zwei ganze Zahlen* $k, l \in \mathbb{Z}$ *gibt mit* $k \cdot x + l \cdot N = 1$.

*Abgabe am 24.6.2013 im Hörsaal vor Beginn der Vorlesung*