Technische Universität München
Fakultät für Informatik
Lehrstuhl für Informatik 15
Computergraphik & Visualisierung
Prof. Dr. Rüdiger Westermann
Dr. Werner Meixner

Wintersemester 2007/08
Übungsblatt 11
9. Februar 2008

# Diskrete Strukturen

*Abgabetermin: 22. Januar* **vor** *der Vorlesung*

## Hausaufgabe 1 (5 Punkte)

Wir gehen von dem in der Tutoraufgabe 1 von Übungsblatt 10 gegebenen Graphen aus, der die Entfernung zwischen bestimmten Städten beschreibt.

Bestimmen Sie mit dem Algorithmus von Kruskal einen minimalen Spannbaum dieses Graphen.

## Hausaufgabe 2 (5 Punkte)

Wir gehen wieder von dem in der Tutoraufgabe 1 von Übungsblatt 10 gegebenen Graphen aus, der die Entfernung zwischen bestimmten Städten beschreibt. Wir nehmen zusätzlich an, dass durch einen Unfall die Verbindung von Nürnberg nach München in beiden Richtungen gesperrt ist.

Bestimmen Sie nun nach dem Algorithmus von Dijkstra die durch den entsprechend modifizierten Verbindungsgraphen gegebene Entfernung zwischen München und Köln.

## Hausaufgabe 3 (5 Punkte)

Sei $S' = \langle S, \circ \rangle$ eine Halbgruppe. Dann nennen wir ein Element $x \in S$ vertauschbar in $S'$, falls gilt $(\forall a \in S)\,[\,a \circ x = x \circ a]$. Es sei $V(S')$ die Menge aller in $S'$ vertauschbarer Elemente von $S$.

Zeigen Sie, dass $V(S')$ eine Unterhalbgruppe von $S'$ erzeugt.

## Hausaufgabe 4 (5 Punkte)

Sei $M = \langle S, \circ \rangle$ ein Monoid mit neutralem Element 1. Wir nehmen an, dass für alle $x \in S$ gilt $x \circ x = 1$.

Zeigen Sie, dass $M$ abelsch ist, d. h., es gilt

$$\forall x, y \in S : x \circ y = y \circ x\,.$$

***Hinweis:*** *Die im Folgenden als* Vorbereitung *bezeichneten Aufgaben werden nicht bewertet und dienen der häuslichen Vorbereitung der Tutoraufgaben, die ebenfalls nicht bewertet werden. Die Abgabe einer Bearbeitung der Vorbereitungsaufgaben zusammen mit der Bearbeitung der Hausaufgaben wird empfohlen. Tutoraufgaben werden in den Übungsgruppen bearbeitet.*

## Vorbereitung 1

Ganze Zahlen $a, b \in \mathbb{Z}$ nennt man kongruent modulo $m$, mit $m \in \mathbb{N}$, i. Z. $a \equiv b \pmod{m}$, falls sich $a$ und $b$ um ein ganzzahliges Vielfaches von $m$ unterscheiden, d. h., falls es ein $k \in \mathbb{Z}$ gibt, so dass $a = b + k \cdot m$ gilt. Genau dann wenn $a \equiv b \pmod{m}$ und gleichzeitig $0 \leq b < m$ gilt, dann gilt $b = a \bmod n$. Diesen Zusammenhang kann man der Definition der Operation mod zugrunde legen.
In enger Beziehung zur mod-Operation steht die ganzzahlige Division $a$ div $m$ zweier Zahlen $a \in \mathbb{Z}, m \in \mathbb{N}$. Es gilt

$$a = (a \text{ div } m) \cdot m + (a \bmod m)\,.$$

1. Zeigen Sie: (i) $5 \text{ div } 2 = 2$, (ii) $(-5) \text{ div } 2 = -3$.
2. Zeigen Sie: Für alle $a \in \mathbb{Z}, m \in \mathbb{N}$ gilt
$$a \text{ div } m = \max\{k \in \mathbb{Z} \mid k \cdot m \leq a\}\,.$$
3. Zeigen Sie die folgende, für den Beweis von Gleichungen modulo einer natürlichen Zahl $m$ nützliche Kennzeichnung der Gleichheit von Zahlen $x, y$.

   Für alle ganzen Zahlen $x, y$ mit $0 \leq x, y < m$ gilt:
$$x = y \quad \Longleftrightarrow \quad x \equiv y \pmod{m}\,.$$

## Vorbereitung 2

Zeigen Sie für alle $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$:

$$\begin{aligned} a &\equiv a \bmod m \pmod{m}\,, \\ (a+b) \bmod m &= [(a \bmod m) + (b \bmod m)] \bmod m\,. \end{aligned}$$

## Vorbereitung 3

Zeigen Sie, dass im Folgenden Algebren $A = \langle S, \circ \rangle$ definiert werden, die bezüglich dem binären Operator $\circ$ eine Gruppe bilden.

1. Sei $S = \mathbb{R} \setminus \{-1\}$ und für alle $x, y \in S$
$$x \circ y = x + y + xy.$$
2. Sei $S$ gleich der Potenzmenge $\mathcal{P}(X)$ $(= 2^X)$ einer beliebigen Menge $X$ und sei $\circ$ gegeben durch
$$A \circ B = (A \cup B) \setminus (A \cap B).$$
3. Sei $1 < n \in \mathbb{N}$ und $S = Z_n^* = \{p \in \mathbb{Z}_n \mid \mathrm{ggT}(p, n) = 1\}$. $\circ$ sei gleich der Multiplikation ganzer Zahlen modulo $n$.

## Tutoraufgabe 1

Die folgenden Aufgaben stützen sich auf die entsprechenden Vorbereitungsaufgaben.

1. Zeigen Sie für alle $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$

$$(a \cdot b) \bmod m \quad = \quad [(a \bmod m) \cdot (b \bmod m)] \bmod m\,.$$

2. Berechnen Sie $(10^{17} + 5^{23} - 30^{100}) \bmod 3$!

3. Bestimmen Sie $2^{7346790100} \bmod 12$!

## Tutoraufgabe 2

Zeigen Sie: Die Menge aller Elemente endlicher Ordnung in einer abelschen Gruppe bildet eine Untergruppe.

## Tutoraufgabe 3

Beweisen Sie die folgenden Aussagen.

1. Jede zyklische Gruppe ist kommutativ.

2. In jeder zyklischen additiven Gruppe mit ungerader Ordnung ist die Summe aller Elemente gleich ihrem neutralen Element 0.

3. Es gibt keine zyklische additive Gruppe mit gerader Ordnung, in der die Summe aller Elemente gleich dem neutralen Element 0 ist.

4. Es gibt keine Gruppe der Ordnung 13, die eine echte Untergruppe enthält, i. e. eine Untergruppe weder von der Ordnung 13, noch von der Ordnung 1.

5. Ist jede Gruppe der Ordnung 13 kommutativ? Begründung!

*Hinweis*: Eine Gruppe nennt man additiv/multiplikativ, wenn man die Verknüpfung als Summe/Produkt bezeichnen will. Inhaltlich gibt es keinen Unterschied zwischen additiven und multiplikativen Gruppen.