Technische Universität München
Institut für Informatik
Lehrstuhl für Effiziente Algorithmen
Prof. Dr. Ernst W. Mayr

WS 1997/98
Übungsblatt 3
2. Dez. 1997

Diskrete Strukturen I

(Abgabetermin: Dienstag, den 2. Dez. 1997, in der Vorlesung)

Aufgabe 1

Zeigen Sie: Eine Untergruppe H einer (endlichen oder unendlichen) Gruppe G ist Normalteiler von G genau dann, wenn

$$a\,H\,a^{-1} \subseteq H \text{ für alle } a \in G\,.$$

Aufgabe 2

Sei G eine Gruppe, so daß für alle $a \in G$ gilt:

$$a\,a = 1\,.$$

Zeigen Sie, daß G abelsch ist.

Aufgabe 3

Wir betrachten die Menge der Transformationen der Form

$$R_{abcd}(x) = \frac{a \cdot x + b}{c \cdot x + d}$$

von $\mathbb{R} \cup \{\infty, -\infty\}$ nach $\mathbb{R} \cup \{\infty, -\infty\}$, mit $a, b, c, d \in \mathbb{R}$. Zusätzlich definieren wir

$$R_{0,0,0,0}(x) = -\infty \text{ für alle } x \in \mathbb{R} \cup \{\infty, -\infty\}$$

und

$$R_{abcd}(-\infty) = -\infty \text{ für alle } a, b, c, d \in \mathbb{R}.$$

1. Wie ist $R_{abcd}(\infty)$ definiert?
   Hinweis: Eine Inspiration zur Definition findet man in der Analysis.
2. Zeigen Sie, daß die R_{abcd} wie oben angegeben unter Komposition ein Monoid bilden.
3. Unter welchen Einschränkungen für a, b, c, d ist dieses Monoid eine Gruppe?

Aufgabe 4

(a) Zeigen Sie, daß $\{m \in \mathbb{N};\ 0 \le m < n, \mathrm{ggT}(m,n) = 1\}$ mit der Multiplikation mod n als Operation eine Gruppe bildet.

(b) Zeigen Sie, daß $\{m \in \mathbb{N};\ 0 < m < n\}$ mit der Multiplikation mod n genau dann eine Gruppe bildet, wenn n eine Primzahl ist.

Aufgabe 5

Bestimmen Sie mit Hilfe von MAPLE (ohne Verwendung der built-in Funktion `primroot`) ein möglichst kleines erzeugendes Element a von $\mathbb{Z}_{997}^*$ sowie für die ersten 30 Elemente $b \in \mathbb{Z}_{997}^*$ den *diskreten Logarithmus* $\mathrm{dlog}_a b$, mit

$$\mathrm{dlog}_a b := \{r;\ a^r = b \bmod 997\}\ .$$