Zentrum für Technomathematik

Prof. Dr. A. Schmidt
Dipl. math. Dipl. inf. J. Benke

Mathematische Grundlagen der Informatik I

WS 2003/04 — Übung 8 — 16.12.2003
Abgabe: 06.01.2004

Aufgabe 25 (Permutationen) (4 Punkte)

Sei $m \in \mathbb{N}$ und $M = \{1, \ldots, m\}$ die Menge der ersten m natürlichen Zahlen.
Die bijektiven Abbildungen $p : M \to M$ beschreiben *Vertauschungen der Reihenfolge* dieser Zahlen. Eine solche Vertauschung nennt man *Permutation*. Man beschreibt eine Permutation p öfters durch

$$p = \begin{pmatrix} 1 & 2 & 3 & \cdots & m \\ p(1) & p(2) & p(3) & \cdots & p(m) \end{pmatrix}.$$

S_m bezeichne die Menge der Permutatonen von M und $\circ$ die Hintereinanderschaltung von Permutationen, $(p_1 \circ p_2)(x) := p_1(p_2(x))$.

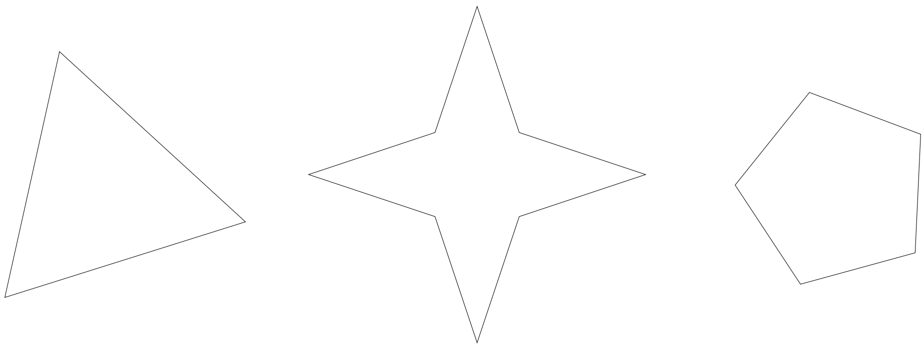
Zeigen Sie, dass $(S_m, \circ)$ eine Gruppe ist.

$(S_m, \circ)$ heißt die *symmetrische Gruppe* mit m Elementen.

Ist $(S_m, \circ)$ eine abelsche Gruppe?

Aufgabe 26 (4 Punkte)

Zeigen Sie, dass die Drehungen, die einen symmetrischen Stern oder ein Polygon mit m Spitzen (so wie unten) in sich überführen, eine Gruppe bilden. (Sie ist isomorph zu $\mathbb{Z}/m\mathbb{Z}$.)



<u>Siehe Seite 2 zur Definition von Ring und Polynomring</u>

Aufgabe 27 (Restklassenring) (4 Punkte)

Sei $m \in \mathbb{N}$. Zeigen Sie, dass $(\mathbb{Z}/m\mathbb{Z}, \oplus, \otimes)$ ein kommutativer Ring ist.

Aufgabe 28 (Polynomring) (4 Punkte)

Sei $(R, +, \cdot)$ ein kommutativer Ring.
Beweisen Sie, dass dann $(R[X], +, \cdot)$ ein kommutativer Ring ist.
Zeigen Sie dazu zunächst, dass durch die entsprechenden punktweisen Verknüpfungen zwei Abbildungen $+ : R[X] \times R[X] \to R[X]$ und $\cdot : R[X] \times R[X] \to R[X]$ definiert werden.

4.6 Definition
Ein **Ring** ist ein Tripel $(R, \oplus, \otimes)$ bestehend aus einer Menge R und zwei Verknübfungen $\oplus, \otimes$ auf R, für die folgende Eigenschaften gelten:

(R1) $(R, \oplus)$ ist eine kommutative Gruppe,

(R2) $(R, \otimes)$ ist assoziativ, das heißt $a \otimes (b \otimes c) = (a \otimes b) \otimes c$ für alle $a, b, c \in R$,

(R3) $(R, \oplus, \otimes)$ ist distributiv, das heißt für alle $a, b, c \in R$ gilt $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ und $a \oplus (b \otimes c) = (a \oplus b) \otimes (a \oplus c)$.

Falls zusätzlich gilt

(R4) $(R, \otimes)$ ist kommutativ, das heißt $a \otimes b = b \otimes a$ für alle $a, b \in R$,

so heißt $(R, \oplus, \otimes)$ ein **kommutativer Ring**.

4.8 Definition
Sei $(R, +, \cdot)$ ein Ring und $a_0, a_1, \dots, a_n \in R$. Die Abbildung

$$p : R \to R, \qquad x \mapsto a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

heißt **Polynom über** R.
Ist $a_n \neq 0$ ($0 =$ neutrales Element bzgl. $+$), so heißt n der **Grad** von p.

4.9 Definition
Sei $(R, +, \cdot)$ ein Ring. Die Menge aller Polynome über R wird mit $R[X]$ bezeichnet. Mit den punktweisen Verknüpfungen

$$(p + q)(x) := p(x) + q(x), \qquad (p \cdot q)(x) := p(x) \cdot q(x)$$

heißt $(R[X], +, \cdot)$ der **Polynomring über** R.