Zentrum für Technomathematik

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

Mathematische Grundlagen der Informatik I

WS 2003/04 — Übung 9 — 06.01.2004
Abgabe: 13.01.2004

Zur Definition von Ringen (Achtung: Berichtigung!) und Körpern siehe Seite 2.

Aufgabe 29 (Rechnen in Restklassenringen/-körpern) (4 Punkte)

a) Lösen Sie in $\mathbb{Z}/4\mathbb{Z}$ die Gleichungen $3 + x = 1$ und $2 - y = 3$.

b) Lösen Sie in $\mathbb{Z}/7\mathbb{Z}$ die Gleichungen $3 + a = 1$, $3 - b = 4$, $3 \cdot c = 1$ und $3 \cdot d = 2$.

c) Bestimmen Sie in $\mathbb{Z}/5\mathbb{Z}$ und $\mathbb{Z}/6\mathbb{Z}$ alle Lösungen der Gleichung $2 \cdot x = 4$.

Aufgabe 30 (Rechnen in Polynomringen) (4 Punkte)

Seien $r(x) = 2x^2 + 2x + 3$ und $s(x) = x^3 + 2$.

a) Berechnen Sie in $(\mathbb{Z}/4\mathbb{Z})(X)$ das Produkt $p = r \cdot s$.

b) Lösen Sie in $(\mathbb{Z}/4\mathbb{Z})(X)$ die Gleichung $r + q = s$.

Aufgabe 31 (Restklassenkörper) (4 Punkte)

a) Überprüfen Sie, dass $(\mathbb{Z}/7\mathbb{Z}, \oplus, \otimes)$ ein Körper ist.

b) Zeigen Sie (durch Gegenbeispiel), dass $(\mathbb{Z}/6\mathbb{Z}, \oplus, \otimes)$ **kein** Körper ist.

Aufgabe 32 (4 Punkte)

Zeigen Sie, dass die komplexen Zahlen $(\mathbb{C}, +, \cdot)$ einen Körper bilden. Die Addition bzw. Multiplikation zweier komplexer Zahlen $a + ib$ und $c + id$ sind dabei definiert als

$$(a + ib) + (c + id) = (a + c) + i(b + d), \qquad (a + ib) \cdot (c + id) = (ac - bd) + i(ad + bc).$$

4.6 Definition — Berichtigung, siehe (R3)
Ein **Ring** ist ein Tripel $(R, \oplus, \otimes)$ bestehend aus einer Menge R und zwei Verknüpfungen $\oplus, \otimes$ 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 $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$.

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**.

4.10 Definition
Ein **Körper** ist ein Tripel $(K, \oplus, \otimes)$ bestehend aus einer Menge K und zwei Verknüpfungen $\oplus, \otimes$ auf K mit folgenden Eigenschaften:

(K1) $(K, \oplus, \otimes)$ ist ein kommutativer Ring.

(K2) Es gibt ein Element 1 („Einselement“) in K mit $\quad 1 \otimes a = a \quad$ für alle $a \in K$.

(K3) Für jedes $a \in K \setminus \{0\}$ gibt es genau ein Element $a^{-1} \in K$ mit $\quad a^{-1} \otimes a = 1$.
Dabei bezeichnet $0 \in K$ das neutrale Element zu $\oplus$ (das „Nullelement“).