Logik und diskrete Stukturen

Felix (2807144) & Philipp (2583572) Müller

WS 14/15

Blatt 9

Aufgabe 1

- $(\mathbb{Z}/5\mathbb{Z}, \odot)$

  a)

$\odot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

  b) Die Auswertungsreihenfolge ist egal, dies ist an der Verknüpfungstafel leicht ersichtlich, daher haben wir Assoziativität. Kommutativität folgt aus der Symmetrie der Verknüpfungstafel gegenüber ihrer Diagonale.

  c) Invertierbare Elemente sind 1 und -1

- $(\mathbb{Z}/6\mathbb{Z}, \odot)$

  a)

$\odot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

  b) analog zu $\mathbb{Z}/5\mathbb{Z}$

  c) $1, -1, 5, -5$

Aufgabe 2

$(R, +, \cdot)$ kommutativer Ring mit 0 als neutrales Element der Addition und 1 als neutrales Element der Multiplikation und $1 \in R$ und $1 \neq 0$.

a) Zu zeigen: $a \in R : (-1) \cdot a = -a$.

Sei r das neutrale Element zur Multiplikation. Dann können wir mit $a \in R$ umformen:

$$(-1) \cdot a = (-n) \cdot a$$

Weil $(R, +, \cdot)$ kommutativer Ring ist können wir wir schreiben

$$= -(n) \cdot a = -n \cdot a = -a$$

Die letzte Gleichheit folgt aus der Definition des neutralen Elements.

b) Zu zeigen: $a, r \in R^* :\ a \cdot r = a \implies r = 1$.

Wir wissen aus $a, r \in R^*$, dass a und r invertierbar sind. Daher haben wir die Eindeutigkeit, die in c) fehlen wird, da $0 \notin R^*$. r muss dann also das neutrale Element darstellen, wenn $a \cdot r = a$ gelten soll. Aus der Aufgabenstellung wissen wir, dass das neutrale Element der Multiplikation eben 1 ist, daher gilt $r = 1$.

c) Zu zeigen: $a, r \in R^* :\ a \cdot r = a \not\Longrightarrow r = 1$.

Betrachten wir $a = 0$ so gilt für jedes r, dass $a \cdot r = a$. Somit können wir nicht $r = 1$ für alle $a, r \in R$ schließen.

d) Zu zeigen: $a, b \in R :\ a \cdot b = 0 \not\Longrightarrow a + 1 \vee b + 1$ sind Einheit.

Würden wir $R = \mathbb{Z}$ wählen würde dies halten, da auf $\mathbb{Z}$ keine Nullteiler existieren (also solche $a \neq 0$ für die es ein b gibt so, dass $a \cdot b = 0$).

Da diese über beliebigen Körpern existieren können wir von $a \cdot b = 0$ nicht folgern, dass $a + 1$ oder $b + 1$ Element sind, wie dies möglich wäre, wenn wir wüssten, dass eines der beiden gleich 0 sein muss und 1 Element ist.

e) $a \in R :\ a \cdot a = 0 \implies a + 1$ ist Einheit.

Die einzige Möglichkei für $a \cdot a = 0$ ist $a = 0$, da Nullteiler nur für $a, b :\ a \neq b$ existieren. Es gilt $0 + 1 = 1$ und $1 \cdot 1 = 1$, es ist also $x \cdot r = e$ erfüllt und es gilt daher, dass $1 \in R^*$.

Aufgabe 3

$x_0 := 8778, x_1 := 3230$

a) Primfaktorzerlegung: Teile durch Primzahlen beginnend mit 2. Rekursiv angewendet ergibt sich:

$$8778 = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 19$$
$$3230 = 2 \cdot 5 \cdot 17 \cdot 19$$

Gemeinsame Primfaktoren: 2 und 19, also ist $ggT(8778, 3230) = 2 \cdot 19 = 38$.

b) Euklid:

$$\begin{aligned} x_{i+1} &: = x_{i-1} \bmod x_i \\ x_2 &= 8778 \bmod 3230 = 2318 \\ x_3 &= 912 \\ x_4 &= 494 \\ x_5 &= 418 \\ x_6 &= 76 \\ x_7 &= 38 \\ x_8 &= 0 \end{aligned}$$

Alos ist $ggT(8778, 3230) = x_7 = 38$.

Aufgabe 4

Wenn wir den euklidischen Algorithmus auf f_{k+1}, f_k anwenden, also $\mathrm{ggT}(f_{k+1}, f_k)$ suchen haben wir

$$
\begin{aligned}
f_{k+1} &= 1 \cdot f_k + f_{k-1} \\
f_k &= 1 \cdot f_{k-1} + f_{k-2} \\
f_{k-1} &= 1 \cdot f_{k-2} + f_{k-3} \\
&\vdots \\
f_4 &= 1 \cdot f_3 + f_2 \\
f_3 &= 2 \cdot f_2 + 0
\end{aligned}
$$

Der letzte Term gilt, da $3 = f_3 = 2 \cdot f_2$, da $f_2 = 1$. Damit terminiert der Algorithmus nach f_3 und wir haben $k + 1 - 2 = k - 1$ Iterationen.