Universität Siegen
Lehrstuhl Theoretische Informatik

Carl Philipp Reh
Daniel König

Diskrete Mathematik für Informatiker

WS 2016/2017

Übung 13

1. Zeigen Sie, dass jeder Körper auch ein Ring ist.

2. Geben Sie einen Körper mit vier Elementen an.

3. Beweisen oder widerlegen Sie: Für einen Ring $(R, +, \cdot)$ gilt:

   a) $\forall a \in R. a \cdot 0 = 0 \cdot a = 0$

   b) $\forall a, b \in R. a \cdot b = 0 \Rightarrow (a = 0 \vee b = 0)$

   c) $\forall a \in R : -a = (-1) \cdot a$

4. Berechnen Sie für die folgenden Polynome $p(x)$ div $q(x)$, $p(x)$ mod $q(x)$ und den ggT der beiden Polynome:

   a) $\begin{aligned} p(x) &= -3x^3 - 13x^2 + 15x + 25 \\ q(x) &= 9x^3 - 21x^2 - 5x + 25 \end{aligned}$

   b) $\begin{aligned} p(x) &= -20x^6 + x^5 - 42x^4 + 10x^3 - 49x^2 - 6x - 24 \\ q(x) &= -20x^3 - 15x^2 - 30x \end{aligned}$

   c) $\begin{aligned} p(x) &= x^3 - 3x^2 + 5x - 3 \\ q(x) &= x^3 - 1 \end{aligned}$

Lösung zu Übung 13

1. Sei $(A, \oplus, \odot)$ ein Körper, wobei 0 das neutrale Element von $\oplus$ und 1 das neutrale Element von $\odot$ ist.

- Nach Voraussetzung ist $A \setminus \{0\}$ eine abelsche Gruppe mit neutralem Element 1, also auch ein Monoid. Um zu zeigen, dass auch $(A, \odot)$ ein Monoid mit neutralem Element 1 ist, müssen wir zeigen, dass die entsprechenden Eigenschaften auch für 0 gelten. Es gilt $0 \odot 1 = 1 \odot 0 = 0$, also ist 1 auch neutral bezüglich 0. Die Assoziativität gilt ebenfalls, denn $a \odot (b \odot c) = 0 = (a \odot b) \odot c$, falls $a = 0$, $b = 0$ oder $c = 0$.
- Um das zweite Distributivgesetz zu beweisen, zeigen wir zunächst, dass $(A, \odot)$ ein kommutatives Monoid ist. Dies gilt, da $(A \setminus \{0\}, \odot)$ eine abelsche Gruppe ist und $a \odot b = b \odot a = 0$, falls $a = 0$ oder $b = 0$. Somit gilt durch Anwenden des ersten Distributivgesetzes, dass

$$\begin{aligned}(b \oplus c) \odot a &= a \odot (b \oplus c) \\ &= (a \odot b) \oplus (a \odot c) \\ &= (b \odot a) \oplus (c \odot a)\end{aligned}$$

2. $GF(p^r)$ für eine Primzahl p und ein $r > 0$ ist ein Körper mit p^r Elementen. Wir wählen $p = r = 2$. Diesen Körper kann man als $\mathbb{F}_p[x]_{a(x)}$ für ein irreduzibles Polynom $a(x) \in \mathbb{F}_p[x]$ vom Grad r erhalten. Konkret ist dies $\mathbb{F}_2[x]_{q(x)}$ mit $q(x) = x^2+x+1$: $q(x)$ ist irreduzibel in $\mathbb{F}_2[x]$, da es keine Nullstellen hat, denn $q(0) = q(1) = 1$. Der so definierte Körper besitzt die vier Elemente 0, 1, x und $x + 1$.

3. Sei $(R, \oplus, \odot)$ ein Ring.

   a) $\forall a \in R. a \odot 0 = 0 \odot a = 0$ gilt auch in Ringen mit derselben Argumentation wie in der Vorlesung:

   $$0 \oplus (a \odot 0) = a \odot 0 = a \odot (0 \oplus 0) = (a \odot 0) \oplus (a \odot 0),$$

   d.h.

   $$0 \oplus ((a \odot 0) \oplus -(a \odot 0)) = (a \odot 0) \oplus ((a \odot 0) \oplus -(a \odot 0))$$

   und somit $0 = (a \odot 0)$.

   b) $\forall a, b \in R. a \cdot b = 0 \Rightarrow (a = 0 \vee b = 0)$ gilt nicht in Ringen. Betrachte z.B. $(\mathbb{Z}_4, +_4, \cdot_4)$, wo $2 \cdot_4 2 = 0$ gilt, aber $2 \neq 0$.

c) $\forall a \in R : -a = (-1) \cdot a$ gilt auch in Ringen mit derselben Argumentation wie in der Vorlesung:

$$a \oplus ((-1) \odot a) = (1 \odot a) \oplus ((-1) \odot a) = (1 \oplus (-1)) \odot a = 0 \odot a = 0$$

Also muss $((-1) \odot a) = -a$ gelten, da es nur ein Element $-a \in R$ gibt mit $a \oplus -a = 0$.

4. Siehe extra Blatt.