4. Übungsblatt

LINEARE ALGEBRA I (WS 2004/05)

Lösungen

9. Aufgabe: In Aufgabe 2 wurde bewiesen: Zu beliebigen ganzen Zahlen a und n mit $n > 0$ gibt es ganze Zahlen q und r mit folgenden Eigenschaften

$$a = qn + r \quad \text{und} \quad 0 \leq r < n$$

(Diese Zahlen q und r sind dadurch sogar eindeutig bestimmt). Man bezeichnet diesen Sachverhalt als "Division mit Rest in $\mathbb{Z}$" und nennt r den "Rest bei Division von a durch n". Man schreibt auch $r =: a \bmod n$.

Auf der Menge $\mathbb{Z}_n := \{0, 1, 2, 3, \ldots, n-1\}$ seien eine Addition $\oplus$ und eine Multiplikation $\odot$ definiert durch

$$\boxed{x \oplus y := (x + y) \bmod n \quad , \quad x \odot y := (x \cdot y) \bmod n \quad (x, y \in \mathbb{Z}_n)}$$

a) $(a + kn) \bmod n = a \bmod n$ für alle $a, k \in \mathbb{Z}$

Beweis: Für $r := (a+kn) \bmod n$ gilt $a+kn = qn+r$ mit $0 \leq r < n$. Daraus folgt $a = (q-k)n+r$ mit $0 \leq r < n$. Nach Definition ist damit $r = a \bmod n$, so daß sich die Behauptung ergibt.

b) Für $\oplus$ gilt das Assoziativ–Gesetz

Beweis: Es ist zu zeigen: $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ für alle $x, y, z \in \mathbb{Z}_n$.
Sei $y + z = qn + r$ mit $r = (y + z) \bmod n$ und $x + y = q'n + r'$ mit $r' = (x + y) \bmod n$. Dann ist $y \oplus z = r$ und $x \oplus y = r'$, und es folgt

$$\begin{aligned}
\underline{\underline{x \oplus (y \oplus z)}} &= x \oplus r \\
&= x \oplus (y + z - qn) \\
&= (x + (y + z - qn)) \bmod n \\
&= (x + (y + z)) \bmod n \quad \text{(nach a))} \\
&= \underline{((x + y) + z) \bmod n} \quad \text{(da + auf } \mathbb{Z} \text{ assoziativ ist)}
\end{aligned}$$

$$\begin{aligned}
\underline{\underline{(x \oplus y) \oplus z}} &= r' \oplus z \\
&= (x + y - q'n) \oplus z \\
&= ((x + y - q'n) + z) \bmod n \\
&= \underline{((x + y) + z) \bmod n} \quad \text{(nach a))}
\end{aligned}$$

Daraus ergibt sich die Behauptung.

c) $x \oplus 0 = x$ für alle $x \in \mathbb{Z}_n$

Beweis: Für alle $x \in \mathbb{Z}_n$ gilt $x \bmod n = x$. Es ist nämlich $x = 0 \cdot n + x$ mit $0 \leq x < n$.
Damit folgt: $x \oplus 0 = (x + 0) \bmod n = x \bmod n = x$.

d) Zu $x \in \mathbb{Z}_n$ existiert ein $y \in \mathbb{Z}_n$ mit $x \oplus y = 0$

Beweis: **<u>1. Fall: $x = 0$</u>** Dann ist $y = 0 \in \mathbb{Z}_n$ das gesuchte Element; denn
$0 \oplus y = 0 \oplus 0 = (0 + 0) \bmod n = 0 \bmod n = 0$.
<u>2. Fall: $x \neq 0$</u> Jetzt gilt $1 \leq x \leq n - 1$, woraus $1 \leq n - x \leq n - 1$ folgt, was man leicht mit Hilfe der Regeln für $\leq$ zeigen kann. Setze $y := n - x$. Dann gilt: $\underline{\underline{y \in \mathbb{Z}_n}}$ und
$x \oplus y = x \oplus (n - x) = (x + (n - x)) \bmod n = n \bmod n = 0$ (denn $n = 1 \cdot n + 0$) .

e) Gibt es zu $2 \in \mathbb{Z}_{14}$ ein $x \in \mathbb{Z}_{14}$ mit $2 \odot x = 1$? (Die Antwort ist zu begründen!)

Antwort: Nein!
Beweis: Annahme: Es existiert ein $x \in \mathbb{Z}_{14}$ mit $2 \odot x = 1$, d.h. $1 = 2 \odot x = (2x) \bmod 14$. Dann gibt es ein $q \in \mathbb{Z}$ mit $2x = q \cdot 14 + 1$, oder umgeformt $2 \cdot \underbrace{(x - q \cdot 7)}_{\in \mathbb{Z}} = 1$. Dies ist aber ein Widerspruch; denn auf der linken Seite steht eine **gerade** ganze Zahl und links eine **ungerade**.

Anmerkung: Analog kann gezeigt werden: $\oplus$ ist kommutativ, $\odot$ ist assoziativ und kommutativ, $1 \in \mathbb{Z}_n$ ist neutrales Element bzgl. $\odot$, und es gilt das Distributivgesetz

$$x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$$

Damit erfüllen die Rechenoperationen $\oplus$ und $\odot$ auf $\mathbb{Z}_n$ formal gesehen alle in (1.1) aufgelisteten Eigenschaften der Addition und Multiplikation reeller Zahlen mit **Ausnahme** der Eigenschaft M_4), wie in Teil e) gezeigt wurde. Also ist $(\mathbb{Z}_n, \oplus, \odot)$ kein Körper.

Man sagt: $(\mathbb{Z}_n, \oplus, \odot)$ ist ein **kommutativer Ring**.

---

10. Aufgabe: M, N, P seien Mengen.

a) Beweise: $(M \cap N) \cup P = M \cap (N \cup P) \iff P \subseteq M$

Beweis: Es sind zwei Beweisrichtungen erforderlich:

"$\Longrightarrow$" **Vor:** $(M \cap N) \cup P = M \cap (N \cup P)$, **Beh:** $P \subseteq M$

Zu zeigen ist, daß jedes Element von P auch Element von M ist.
Sei $x \in P$ beliebig. Dann gilt $x \in (M \cap N) \cup P$ nach Definition der Vereinigung. Nach Voraussetzung folgt daraus $x \in M \cap (N \cup P)$ und daraus $x \in M$ nach Definition des Durchschnittes.

"$\Longleftarrow$" **Vor:** $P \subseteq M$, **Beh:** $(M \cap N) \cup P = M \cap (N \cup P)$

$$\begin{aligned} (M \cap N) \cup P &= (M \cup P) \cap (N \cup P) \quad \text{(Distributivgesetz (3.6d))} \\ &= M \cap (N \cup P) \quad (\text{wegen } P \subseteq M \text{ gilt } M \cup P = M \quad (\star)) \end{aligned}$$

$(\star)$ Dies ist die der Aufgabe 6 entsprechende Aussage für die Vereinigung.

b) Welche Teilmengenbeziehung gilt zwischen den Mengen $(M \setminus N) \setminus P$ und $M \setminus (N \setminus P)$? Müssen sie gleich sein? Begründe alle Antworten.

Beweis: Durch Zeichnen eines passenden Mengendiagrammes kommt man zu der Vermutung

$$(\star) \qquad (M \setminus N) \setminus P \subseteq M \setminus (N \setminus P)$$

Zu zeigen: Jedes Element aus $(M \setminus N) \setminus P$ ist auch Element aus $M \setminus (N \setminus P)$.

$$\begin{aligned} x \in (M \setminus N) \setminus P &\implies (x \in M \wedge x \notin N) \wedge x \notin P \\ &\implies x \in M \wedge \underline{x \notin N} \quad (\star\star) \end{aligned}$$

$(\star\star)$ Hier wird die allgemeinrichtige Formel $A \wedge B \Longrightarrow A$ benutzt.

Wir müssen noch zeigen: $x \notin N \setminus P$. Annahme: $x \in N \setminus P$. Dann folgt $x \in N$ im Widerspruch zu $x \notin N$, wie oben gesehen. Folglich gilt $x \in M$ und $x \notin N \setminus P$, insgesamt also $x \in M \setminus (N \setminus P)$. Damit ist $(\star)$ bewiesen.

Mit dem Mengendiagramm kann man auch zu der Vermutung kommen, daß in $(\star)$ nicht immer die Gleichheit gelten muß . Dies müssen wir aber mit einem **konkreten** Beispiel belegen:
Setze $M = \{1, 2\}$, $N = \{1, 3\}$, $P = \{1, 4\}$. Dann ist $(M \setminus N) \setminus P = \{2\}$ und $M \setminus (N \setminus P) = \{1, 2\}$, d.h. in $(\star)$ gilt i.a. **nicht** die Gleichheit.