Lösungsvorschläge zu Aufgabenblatt 8

(Restklassenoperationen)

Aufgabe 8.1

(1) Sei $m \in \mathbb{N}$ mit $m \geqslant 2$ ein fester Modulus. Zeigen Sie, dass Restklassenpotenzieren nicht unabhängig vom Repräsentanten definiert werden kann, d.h.:

$$[a]_m^{[n]_m} := [a^n]_m \quad (a \in \mathbb{Z}, n \in \mathbb{N}_0)$$

ist keine sinnvolle Definition.

(2) Welche der folgenden Definitionen

$$f([a]_3) := [a]_6, \quad g([a]_3) := [2 \cdot a]_6 \qquad (a \in \mathbb{Z})$$

erklärt eine wohldefinierte Abbildung von $\mathbb{Z}_3$ nach $\mathbb{Z}_6$?

Lösung

(1) Wir zeigen zunächst ein einfaches konkretes Beispiel: Sei $m = 2$, für $a = 2$ und $n = 0$ gilt dann $[n]_2 = [0]_2 = [2]_2$, also

$$[2^0]_2 = [1]_2, \text{ aber } [2^2]_2 = [4]_2 = [0]_2 \neq [1]_2.$$

Wegen $[n]_2 = [0]_2 = [2]_2$ ist daher die versuchte Definition von $[a]_2^{[n]_2}$ nicht unabhängig vom Repräsentanten.

Das gleiche Prinzip lässt sich für allgemeines $m \geqslant 2$ anstelle von $m = 2$ anwenden: Dazu betrachten wir $a = m$ und $n = 0$. Dann gilt $[n]_m = [0]_m = [m]_m$. Weiter gilt $[m^0]_m = [1]_m$ und $[m^m]_m = [0]_m$, denn $m | m^m$. Wegen $m \geqslant 2$ ist $[0]_m \neq [1]_m$. Also ist auch im allgemeinen Fall die versuchte Definition von $[a]_m^{[n]_m}$ nicht unabhängig vom Repräsentanten.

(2) Wir zeigen, dass die Definition von g unabhängig vom Repräsentanten ist, die von f hingegen nicht.

f ist nicht wohldefiniert: Es gilt zum Beispiel $[1]_3 = [4]_3$, aber es ist $[1]_6 \neq [4]_6$.

g ist wohldefiniert: Seien $a, b \in \mathbb{Z}$ mit $[a]_3 = [b]_3$, dann gibt es ein $k \in \mathbb{Z}$ mit $a = b + 3k$. Es folgt $2a = 2b + 6k$, also ist auch $[2a]_6 = [2b]_6$.

Aufgabe 8.2

Berechnen Sie folgende Restklassenausdrücke:
$[4]_5 \oplus [6]_5$, $[6999]_7 \oplus [632]_7$, $[4]_{12}^2$, $[10]_{15}^2$, $[12]_{10}^{10}$, $[10]_{12} \otimes [6]_{12}$, $[17]_{15} \otimes [1503]_{15}$.

Lösung

1. $[4]_5 \oplus [6]_5 = [4 + 6]_5 = [10]_5 = [0]_5$,

2. $[6999]_7 \oplus [632]_7 = [-1]_7 \oplus [2]_7 = [1]_7$,
3. $[4]_{12}^2 = [4^2]_{12} = [16]_{12} = [4]_{12}$,
4. $[10]_{15}^2 = [10^2]_{15} = [100]_{15} = [10]_{15}$,
5. $[12]_{10}^{10} = [2]_{10}^{10} = [2^{10}]_1 0 = [1024]_{10} = [4]_{10}$,
6. $[10]_{12} \otimes [6]_{12} = [10 \cdot 6]_{12} = [60]_{12} = [0]_{12}$,
7. $[17]_{15} \otimes [1503]_{15} = [2]_{15} \otimes [3]_{15} = [2 \cdot 3]_{15} = [6]_{15}$.

Aufgabe 8.3

(a) Zeigen Sie, dass eine Quadratzahl bei Division durch 4 nur den Rest 0 oder 1 haben kann.

(b) Folgern Sie, dass die Summe zweier ungerader Quadratzahlen niemals eine Quadratzahl sein kann.

Lösung

(a) Es sei $x \in \mathbb{N}$ eine Quadratzahl, es gibt also ein $a \in \mathbb{Z}$ mit $x = a^2$. Es gilt $[a]_4 \in \{[0]_4, [1]_4, [2]_4, [3]_4\}$. Wegen $[x]_4 = [a^2]_4$ folgt damit

$$[x]_4 \in \{[0^2]_4, [1^2]_4, [2^2]_4, [3^2]_4\} = \{[0]_4, [1]_4, [4]_4, [9]_4\} = \{[0]_4, [1]_4\},$$

und das heißt gerade, dass x nach Division durch 4 den Rest 0 oder 1 hat.

(b) Es sei $y \in \mathbb{N}$ die Summe zweier ungerader Quadratzahlen, also gibt es $a, b \in \mathbb{Z}$ mit $y = a^2 + b^2$ und a^2 und b^2 sind ungerade. Eine ungerade Zahl kann nach Teilen durch 4 nur den Rest 1 oder 3 haben. Mit Teil (a) folgt $[a^2]_4 = [b^2]_4 = [1]_4$, also ist

$$[y]_4 = [a^2 + b^2]_4 = [a^2]_4 \oplus [b^2]_4 = [1]_4 \oplus [1]_4 = [2]_4.$$

Wiederum mit Teil (a) folgt, dass y keine Quadratzahl sein kann, da $[y]_4 \notin \{[0]_4, [1]_4\}$ ist.

Aufgabe 8.4

Auf welche 3 Ziffern endet die Zahl 2^{100}?

Hinweis: *Sie können den NAK-Taschenrechner (TR) zur Hilfe nehmen. Zerlegen Sie dafür* 2^{100} *mithilfe von Potenzrechen-Gesetzen und modulo-Rechnung schrittweise in Zahlen, die der TR berechnen kann.*

Lösung

Wir stellen zunächst fest, dass sich die Aufgabe nicht direkt mit dem TR lösen lässt: Rechnet man diese 30-stellige Zahl auf einem TR aus, so erhält man nur die ersten 8 Ziffern, aber keine Information über die *letzten* Ziffern.

Informationen über diese Ziffern erhält man aber aus der Modulrechnung, denn die letzten drei Ziffern einer Zahl sind gerade deren Rest bei Division durch $m := 1000$. Bei den folgenden Rechnungen leistet ein TR trotzdem gute Dienste. Wir schreiben zuerst $2^{100} = (2^{10})^{10} = 1024^{10}$ und ersetzen $1024 \equiv_m 24$. Dies liefert

$$2^{100} = 1024^{10} \equiv_m 24^{10}.$$

Auch die Zahl 24^{10} kann noch nicht direkt von dem TR berechnet werde, wir schreiben diese daher wieder um:

$$24^{10} = (24^3)^3 \cdot 24.$$

Der TR hilft nun weiter: $24^3 = 13824 \equiv_m 824$, also

$$(24^3)^3 \cdot 24 \equiv_m 824^3 \cdot 24$$

Weiter mit dem TR: $824^3 = 559476224 \equiv_m 224$, also erhalten wir schließlich

$$2^{100} \equiv_m 824^3 \cdot 24 \equiv_m 224 \cdot 24 = 5376 \equiv_m 376.$$

Die Zahl 2^{100} endet also auf die drei Ziffern 376.[1]

Aufgabe 8.5

(a) Erstellen Sie eine Verknüpfungstafel für $(\mathbb{Z}_7\backslash\{0\}, \otimes)$.

(b) Gelten Existenz- und Eindeutigkeitssätze in $(\mathbb{Z}_7\backslash\{0\}, \otimes)$?

(c) Lösen Sie die Gleichung $[4]_7 \otimes x = [6]_7$.

Lösung

(a)

$\otimes$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[5]_7$	$[6]_7$
$[1]_7$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[5]_7$	$[6]_7$
$[2]_7$	$[2]_7$	$[4]_7$	$[6]_7$	$[1]_7$	$[3]_7$	$[5]_7$
$[3]_7$	$[3]_7$	$[6]_7$	$[2]_7$	$[5]_7$	$[1]_7$	$[4]_7$
$[4]_7$	$[4]_7$	$[1]_7$	$[5]_7$	$[2]_7$	$[6]_7$	$[3]_7$
$[5]_7$	$[5]_7$	$[3]_7$	$[1]_7$	$[6]_7$	$[4]_7$	$[2]_7$
$[6]_7$	$[6]_7$	$[5]_7$	$[4]_7$	$[3]_7$	$[2]_7$	$[1]_7$

(b) Da in jeder Zeile und Spalte jedes Element aus $\mathbb{Z}_7\backslash\{0\}$ genau einmal vorkommt, gelten in $(\mathbb{Z}_7\backslash\{0\}, \otimes)$ sowohl ein (beidseitiger) Existenz- als auch Eindeutigkeitssatz (vgl. Prinzipien "Existenzsatz und Verknüpfungstafel" bzw. "Eindeutigkeitssatz und Verknüpfungstafel", VL Folie 142).

[1] Natürlich ist es heute nicht schwer, Software für einen Computer zu finden, die eine solche Zahl exakt berechnet. Man erhält dann $2^{100} = 1267650600228229401496703205376$.

(c) Nach Teil (b) gibt es genau eine Lösung, und in der Verknüpfungstafel lesen wir $[4]_7 \otimes [5]_7 = [6]_7$ ab, also ist $x = [5]_7$ die eindeutige Lösung der Gleichung $[4]_7 \otimes x = [6]_7$.

Aufgabe 8.6

Es sei $m \in \mathbb{N}$ fest. Zeigen Sie, dass in $\mathbb{Z}_m$ das Distributivgesetz gilt, also dass für alle $a, b, c \in \mathbb{Z}$ gilt

$$[a]_m \otimes ([b]_m \oplus [c]_m) = ([a]_m \otimes [b]_m) \oplus ([a]_m \otimes [c]_m).$$

Lösung

Es seien $a, b, c \in \mathbb{Z}$. Wir verwenden die Definition der Restklassenoperationen um die Behauptung auf das Distributivgesetz in$\mathbb{Z}$ zurückzuführen:

$$\begin{aligned} [a]_m \otimes ([b]_m \oplus [c]_m) &= [a]_m \otimes [b+c]_m = [a(b+c)]_m = [ab+ac]_m = [ab]_m \oplus [ac]_m \\ &= ([a]_m \otimes [b]_m) \oplus ([a]_m \otimes [c]_m). \end{aligned}$$

Die folgenden beiden Aufgaben sollen zeigen, wie ähnliche Definitionen von Verknüpfungen wie bei Restklassen dennoch zu nicht-wohldefinierten Abbildungen führen können.

Aufgabe 8.7

Definiere $M := \mathbb{Z} \times \mathbb{N}$, und auf M definiere die Relation

$$(a, b) \equiv (c, d) :\Leftrightarrow ad = bc \quad ((a, b), (c, d) \in M).$$

(a) Zeigen Sie, dass $\equiv$ eine Äquivalenzrelation ist.

(b) Welche der folgenden Definitionen sind unabhängig vom Repräsentanten, definieren also eine Verknüpfung auf $G := M/\equiv$?

$$[(a, b)] \oplus [(c, d)] := [(a + c, b + d)], \quad [(a, b)] \otimes [(c, d)] := [(ac, bd)].$$

Lösung

(a) Seien $(a, b), (c, d), (e, f) \in M$.

$\equiv$ *ist reflexiv:* Es gilt $ab = ba$, also gilt nach Definition $(a, b) \equiv (a, b)$.

$\equiv$ *ist symmetrisch:* Es gelte $(a, b) \equiv (c, d)$. Dann gilt $ad = bc$, also auch $cb = da0$, also gilt nach Definition $(c, d) \equiv (a, b)$.

$\equiv$ *ist transitiv:* Es gelte $(a, b) \equiv (c, d)$ und $(c, d) \equiv (e, f)$. Dann gilt $ad = bc$ und $cf = de$, also auch

$$afc = a(cf) = a(de) = (ad)e = bce = bec. \tag{1}$$

Ist $c = 0$, so folgt aus $ad = bc = 0$ und $d \in \mathbb{N}$ auch $a = 0$, und aus $de = cf = 0$ folgt $e = 0$, also gilt in diesem Fall $af = 0 = be$. Ist $c \neq 0$, so können wir in (1) durch c teilen und erhalten

ebenfalls $af = be$. Damit gilt nach Definition auch $(a, b) \equiv (e, f)$.

(b) Wir zeigen, dass die Verknüpfung $\otimes$ wohldefiniert ist, die Verknüpfung $\oplus$ aber nicht.

Dafür ist als erstes zu zeigen:

$$\forall\,(a,b),(c,d),(a',b'),(c',d') \in M[(a,b)] = [(a',b')] \wedge [(c,d)] = [(c',d')] \Rightarrow [(ac,bd)] = [(a'c',b'd')].$$

Seien $(a, b), (c, d), (a', b'), (c', d') \in M$ mit $(a, b) \equiv (a', b')$ und $(c, d) \equiv (c', d')$. Dann gilt $ab' = a'b$ und $cd' = c'd$, also gilt auch

$$(ac)(b'd') = (ab')(cd') = (a'b)(c'd) = (bd)(a'c').$$

und somit gilt nach Definition auch $(ac, bd) \equiv (a'c', b'd')$. Somit ist $\otimes$ eine wohldefinierte Verknüpfung auf G.

Wir zeigen als nächstes anhand eines Gegenbeispiels, dass die Definition von $\oplus$ nicht unabhängig vom Repräsentanten ist. Wir betrachten dazu $(a, b) = (1, 1)$ und $(c, d) = (1, 2)$, dann ist

$$[(a + c, b + d)] = [(1 + 1, 1 + 2)] = [(2, 3)].$$

Definieren wir $a' := b' = 2$, so gilt wegen $1 \cdot 2 = 2 \cdot 1$, dass $(a, b) \equiv (a', b')$ ist. Andererseits ist aber

$$[(a' + c, b' + d)] = [(2 + 1, 2 + 2)] = [(3, 4)],$$

und wegen $2 \cdot 4 = 8 \neq 9 = 3 \cdot 3$, also $[(2, 3)] \neq [(3, 4)]$.

Anmerkung: *Die Menge G entspricht gerade den rationalen Zahlen: Die Konstruktion zeigt, dass $\equiv$ gerade die Bildgleichheitrelation der Abbildung $f : M \to \mathbb{Q}, (a, b) \mapsto \frac{a}{b}$ ist, es werden also solche Paare aus M identifiziert, die denselben Bruch darstellen. Aus der Bruchrechnung ist nun bekannt, dass die Regel $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ gültig ist, die Regel $\frac{a}{b} + \frac{c}{d} = \frac{a+c}{b+d}$ hingegen nicht, und dies spiegelt sich in der Aufgabe wieder. Eine korrekte Definition der Addition auf G wäre gegeben durch $[(a, b)] \oplus [(c, d)] := [(ad + bc, bd)]$.*

Aufgabe 8.8

Auf $\mathbb{R}$ definiere die Relation

$$x \equiv y :\Leftrightarrow xy > 0 \ \vee \ x = y = 0 \qquad (x, y \in \mathbb{R}).$$

(a) Zeigen Sie, dass $\equiv$ eine Äquivalenzrelation ist.

(b) Welche der folgenden Definitionen sind unabhängig vom Repräsentanten, definieren also eine Verknüpfung auf $M := \mathbb{R}/\equiv$?

$$[x] \oplus [y] := [x + y], \quad [x] \otimes [y] := [xy] \qquad (x, y \in \mathbb{R}).$$

Lösung

(a) Seien $x, y, z \in \mathbb{R}$.

$\equiv$ *ist reflexiv:* Ist $x \neq 0$, so gilt $x \cdot x = x^2 > 0$, also gilt nach Definition $x \equiv x$. Ferner gilt nach Definition auch $0 \equiv 0$.

$\equiv$ *ist symmetrisch:* Es gelte $x \equiv y$. Ist $x = 0$ oder $y = 0$, so folgt $x = y = 0$ und damit auch $y \equiv x$. Es gelte also $x \neq 0$ und $y \neq 0$. Dann gilt $xy >$, also auch $yx = xy > 0$, also gilt nach Definition $y \equiv x$.

$\equiv$ *ist transitiv:* Es gelte $x \equiv y$ und $y \equiv z$. Ist $y = 0$, so gilt auch $x = 0$ und $z = 0$, also $x \equiv z$. Es gelte also $y \neq 0$, dann muss auch $x \neq 0$ und $z \neq 0$ sein. Dann gilt $xy > 0$ und $yz > 0$, also auch $xz = \frac{(xy)\cdot(yz)}{y^2} > 0$, und damit gilt nach Definition auch $x \equiv z$.

(b) Wir bemerken zunächst (auch wenn dies nicht Teil der Aufgabenstellung war): Zwei reelle Zahlen sind offenbar genau dann äquivalent, wenn sie dasselbe Vorzeichen besitzen, oder wenn sie beide gleich 0 sind, also ist $G = \{\mathbb{R}_{<0}, \{0\}, \mathbb{R}_{>0}\} = \{[-1], [0], [1]\}$.

Wir zeigen, dass die Verknüpfung $\otimes$ wohldefiniert ist, die Verknüpfung $\oplus$ aber nicht.

Dafür ist als erstes zu zeigen:

$$\forall\, x, x', y, y' \in \mathbb{R} :\ [x] = [x'] \wedge [y] = [y'] \Rightarrow [xy] = [x'y'].$$

Seien $x, x', y, y' \in \mathbb{R}$ mit $x \equiv x'$ und $y \equiv y'$. Ist $x = 0$, so muss auch $x' = 0$ sein, und es folgt $xy = 0 = x'y'$ und damit insbesondere auch $[xy] = [0] = [x'y']$. Analog folgt $[xy] = [0] = [x'y']$, falls eine der Zahlen x', y, y' gleich 0 ist. Wir nehmen also an, dass $x, x', y, y' \neq 0$ sind. Dann gilt $xx' > 0$ und $yy' > 0$, also auch $(xy)(x'y') = xx'yy' > 0$, also $xy \equiv x'y'$, was zu zeigen war.

Wir zeigen nun, dass die Definition von $\oplus$ nicht unabhängig vom Repräsentanten ist: Zum Beispiel gilt $(-1) + 1 = 0$, aber andererseits ist $[1] = [2]$ und $(-1) + 2 = 1$, aber $[0] \neq [1]$.