Elemente der Mathematik - Sommer 2017

Prof. Dr. Peter Koepke, Thomas Poguntke — Lösung 1

Aufgabe 54 (4+2 Punkte)**.** In der Vorlesung wurde die Multiplikation auf den ganzen Zahlen definiert durch

$$\overline{(a,b)} \cdot \overline{(a',b')} = \overline{(a \cdot a' + b \cdot b', a \cdot b' + b \cdot a')}$$

für natürliche Zahlen $a, a', b, b' \in \mathbb{N}$.

(a) Zeigen Sie, dass diese Operation wohldefiniert ist.

(b) Gilt dies ebenfalls für den folgenden naiven Versuch einer Definition?

$$\overline{(a,b)} \odot \overline{(a',b')} = \overline{(a \cdot a', b \cdot b')}$$

Lösung. (a) Zum Nachweis der Wohldefiniertheit muss man nachprüfen, dass falls $\overline{(a,b)} = \overline{(c,d)}$ und $\overline{(s,t)} = \overline{(p,q)}$, auch $\overline{(a,b)} \cdot \overline{(s,t)} = \overline{(c,d)} \cdot \overline{(p,q)}$ gelten muss.

Sei also $\overline{(a,b)} = \overline{(c,d)}$ und $\overline{(s,t)} = \overline{(p,q)}$. Zu zeigen ist, dass:

$$\overline{(a \cdot s + b \cdot t, a \cdot t + b \cdot s)} = \overline{(c \cdot p + d \cdot q, c \cdot q + d \cdot p)}$$

Dies ist äquivalent zu der Aussage, dass

$$a \cdot s + b \cdot t + c \cdot q + d \cdot p = c \cdot p + d \cdot p + a \cdot t + b \cdot s$$

Ohne Einschränkung lässt sich annehmen, dass $b \leq a$, somit gibt es ein $k \in \mathbb{N}$, sodass $b + k = a$ gilt. Da wegen $\overline{(a,b)} = \overline{(c,d)}$ die Gleichung $a + d = b + c$ gilt, folgt, dass $d + k = c$ gelten muss. Außerdem gilt wegen $\overline{(s,t)} = \overline{(p,q)}$, dass $s + q = p + t$ ist.

Nun ist

$$\begin{aligned}
& a \cdot s + b \cdot t + c \cdot q + d \cdot p \\
&= (b+k) \cdot s + b \cdot t + (d+k) \cdot q + d \cdot q \\
&= b \cdot s + k \cdot s + b \cdot t + d \cdot q + k \cdot q + d \cdot p \\
&= b \cdot s + b \cdot t + d \cdot q + d \cdot p + k \cdot (s+q) \\
&= b \cdot s + b \cdot t + d \cdot q + d \cdot p + k \cdot (p+t) \\
&= b \cdot s + d \cdot p + (b+k) \cdot t + (d+k) \cdot p \\
&= b \cdot s + d \cdot p + a \cdot t + c \cdot p \\
&= c \cdot p + d \cdot p + a \cdot t + b \cdot s
\end{aligned}$$

Die Gleichheit des ersten und letzten Terms zeigt die Wohldefiniertheit.

(b) Die Operation $\odot$ ist nicht wohldefiniert, denn $\overline{(1,0)} = \overline{(1,0)}$ und $\overline{(1,1)} = \overline{(0,0)}$, aber

$$\overline{(1,0)} \odot \overline{(1,1)} = \overline{(1,0)} \neq \overline{(0,0)} = \overline{(1,0)} \odot \overline{(0,0)}$$

Dies ist ein Gegenbeispiel.

Aufgabe 55 (2+2+3 Punkte)**.** Sei $n \geq 1$ eine natürliche Zahl.

(a) Für zwei ganze Zahlen $a, b \in \mathbb{Z}$ schreiben wir

$$a \equiv b \bmod n$$

falls a und b denselben Rest bei der Division durch n haben. Zeigen Sie, dass dies äquivalent zu $n \mid (a - b)$ ist.

(b) Zeigen Sie, dass $\equiv$ eine Äquivalenzrelation auf $\mathbb{Z}$ definiert.

Definition: Wir bezeichnen die Äquivalenzklasse von $a \in \mathbb{Z}$ mit

$$(a + n\mathbb{Z}) = \{b \in \mathbb{Z} \mid b \equiv a \bmod n\},$$

und die Menge der Äquivalenzklassen mit $\mathbb{Z}/n\mathbb{Z} = \{(a + n\mathbb{Z}) \mid a \in \mathbb{Z}\}$.

(c) Beweisen Sie, dass jede Äquivalenzklasse genau ein a mit $0 \leq a < n$ enthält, und demnach die Abbildung

$$\{0, \ldots, n-1\} \longrightarrow \mathbb{Z}/n\mathbb{Z},\ a \longmapsto (a + n\mathbb{Z}),$$

bijektiv ist. Folgern Sie, dass die b-adische Darstellung eine Bijektion

$$\{(z_{k-1}, \ldots, z_0) \in \{0, \ldots, b-1\}^k \mid\ (z_{k-1}, \ldots, z_0) \neq 0\} \longrightarrow \mathbb{Z}/(b^k - 1)\mathbb{Z}$$

liefert, für fest gewählte natürliche Zahlen $b \geq 2$ und $k \geq 1$.

Bemerkung: Für kleine n ist $\mathbb{Z}/n\mathbb{Z}$ bereits aus der Vorlesung bekannt. Zum Fall $n = 1$ ist laut (c) nicht viel zu sagen. Die Gruppe $\mathbb{Z}/2\mathbb{Z}$ ist auf Präsenzblatt 12, Aufgabe 1, und sowohl im Kontext von Wahrheitswerten als auch der Binärzahlen aufgetaucht, und $\mathbb{Z}/3\mathbb{Z}$ kennen Sie aus Aufgabe 53.

Lösung. Im Folgenden sei, wenn eine Zahl $a \in \mathbb{N}$ als $a = qn + r$ dargestellt wird, immer die nach **Lemma 83** eindeutige Darstellung mit $0 \leq r < n$ gemeint.

(a) ($\Rightarrow$) Es haben a und b den selben Rest modulo n, also $a = qn + r$ und $b = tn + r$ für $q, t \in \mathbb{Z}$. Dann ist $a - b = (qn + r) - (tn + r) = (q - t)n + r - r = (q - t)n$. Also $n \mid (a - b)$ (und somit auch $n \mid (b - a)$).

($\Leftarrow$) Es gelte, dass $n \mid (a-b)$, also $sn = a - b$ für geeignetes $s \in \mathbb{Z}$. Sei a darstellbar in der Form $a = qn + r$, dann gilt:

$$b = a - (a - b) = qn + r - sn = (q - s)n + r$$

Da $q - s \in \mathbb{Z}$ ist und $0 \leq r < n$ haben a und b den selben Rest nach Division mit n.

(b) Da $n \mid 0$ und $n \mid m \to n \mid -m$ und $n \mid a \wedge n \mid b \to n \mid a + b$ gelten, folgt aus Aufgabenteil (a), dass $\equiv$ eine Äquivalenzrelation ist.

(c) Existenz: Sei $(a + n\mathbb{Z})$ eine beliebige Äquivalenzklasse. Da a als $a = qn + r$ dargestellt werden kann und dann $a \equiv r \bmod n$ gelten muss, ist die Existenz gezeigt. r erfüllt die Bedingungen.
Eindeutigkeit: Seien r und s beide in $(a + n\mathbb{Z})$ mit $0 \leq r, s < n$. Dann sind für sowohl $a = qn + r$ als auch $a = tn + s$ gültige Darstellungen für a, da a zu r und s in Relation ist. Auf Grund von Lemma 83 sind diese Darstellungen aber eindeutig. Also gilt $r = s$.
Zunächst ist die b-adische Darstellung eine Abbildung

$$f : \{(z_{k-1}, \ldots, z_0) \in \{0, \ldots, b-1\}^k \mid (z_{k-1}, \ldots, z_0) \neq (0, \ldots, 0)\} \longrightarrow \{1, \ldots, b^k - 1\},$$

denn

$$f(z_{k-1}, \ldots, z_0) = \sum_{i=0}^{k-1} z_i \cdot b^i \geq 1,$$

da $(z_{k-1}, \ldots, z_0) \neq (0, \ldots, 0)$ und

$$\begin{aligned} f(z_{k-1}, \ldots, z_0) &= \sum_{i=0}^{k-1} z_i \cdot b^i \\ &\leq \sum_{i=0}^{k-1} (b-1) \cdot b^i \\ &= (b-1) \cdot \sum_{i=0}^{k-1} b^i \\ &\overset{geom.Reihe(b\neq 1)}{=} (b-1) \cdot \frac{b^k - 1}{b-1} \\ &= b^k - 1 \end{aligned}$$

Da sowohl die Menge $\{(z_{k-1}, \ldots, z_0) \in \{0, \ldots, b-1\}^k \mid (z_{k-1}, \ldots, z_0) \neq (0, \ldots, 0)\}$ als auch $\{1, \ldots, b^k - 1\}$ beide die Kardinalität $b^k - 1$ haben und f nach Lemma 85 injektiv ist, folgt, dass f schon eine Bijektion sein muss. Nach dem ersten Teil von Aufgabe (c) gibt dies daher auch eine Bijektion

zwischen $\{(z_{k-1},\dots,z_0)\in\{0,\dots,b-1\}^k \mid (z_{k-1},\dots,z_0)\neq(0,\dots,0)\}$ und $\mathbb{Z}/(b^k-1)\mathbb{Z}$.

Aufgabe 56 (3+4+2 Punkte)**.** Sei $n\geq 1$ eine natürliche Zahl.

(a) Zeigen Sie, dass die Addition und Multiplikation $\mathbb{Z}/n\mathbb{Z}$ mit wohldefinierten Strukturen ausstatten, vermöge

$$(a+n\mathbb{Z})+(b+n\mathbb{Z})=(a+b+n\mathbb{Z})$$

$$(a+n\mathbb{Z})\cdot(b+n\mathbb{Z})=(a\cdot b+n\mathbb{Z})$$

Leiten Sie aus der bekannten Tatsache für $\mathbb{Z}$ ab, dass $(\mathbb{Z}/n\mathbb{Z},+,(0+n\mathbb{Z}))$ eine Gruppe ist.

Bemerkung: Diese wird die zyklische Gruppe (von Ordnung n) genannt.

(b) Bestimmen Sie alle natürlichen Zahlen $d\in\mathbb{N}$, für welche die Abbildung

$$\rho\colon \mathbb{Z}/n\mathbb{Z}\longrightarrow\mathbb{Z}/d\mathbb{Z},\ (a+n\mathbb{Z})\longmapsto(a+d\mathbb{Z}),$$

wohldefiniert ist. In diesem Fall, zeigen Sie, dass ρ sowohl die additive als auch die multiplikative Struktur erhält, und bestimmen Sie die Kardinalität

$$|\rho^{-1}(\{0+d\mathbb{Z}\})|.$$

(c) Finden Sie die Lösungsmenge aller $a\in\mathbb{Z}$ für das Gleichungssystem

$$a\equiv 2 \bmod 9$$

$$a\equiv 3 \bmod 7$$

Hinweis: $4\cdot 7-3\cdot 9=1$.

Lösung. (a) Sei $(a+n\mathbb{Z})=(c+n\mathbb{Z})$ und $(b+n\mathbb{Z})=(d+n\mathbb{Z})$, das heißt

$$a=qn+r, b=pn+s, c=tn+r, d=mn+s$$

für geeignete $q,p,t,n\in\mathbb{Z}$. Daraus folgt, dass

$$a+b=qn+r+pn+s\equiv r+s \bmod n$$
$$c+d=tn+r+mn+s\equiv r+s \bmod n$$

$r+s$ muss dabei <u>nicht</u> $<n$ sein!
Da aber nach Aufgabe 55(b) $\equiv$ eine Äquivalenzrelation ist, gilt

$$a+b\equiv r+s\equiv c+d \bmod n$$

und somit $a + b \equiv c + d \bmod n$.
Die Rechnung für die Multiplikation erfolgt analog.
Seien a, b, c, d wie oben. Es gilt

$$\begin{aligned} a \cdot b = (qn + r) \cdot (pn + s) &= qpn^2 + rpn + sqn + rs \\ &= (qpn + rp + sq) \cdot n + rs \equiv rs \bmod n \\ c \cdot d = (tn + r) \cdot (mn + s) &= tmn^2 + rmn + stn + rs \\ &= (tmn + rm + st) \cdot n + rs \equiv rs \bmod n \end{aligned}$$

Beide sind äquivalent zu $r \cdot s$ und somit auch zueinander.
zz: $(\mathbb{Z}/n\mathbb{Z}, +, (0 + n\mathbb{Z}))$ ist eine Gruppe.

$$\begin{aligned} &((a + n\mathbb{Z}) + (b + n\mathbb{Z})) + (c + n\mathbb{Z}) \\ &= ((a + b) + n\mathbb{Z}) + (c + n\mathbb{Z}) \\ &= (((a + b) + c) + n\mathbb{Z}) \\ &\overset{\mathbb{Z}\ Gruppe}{=} ((a + (b + c)) + n\mathbb{Z}) \\ &= (a + n\mathbb{Z}) + ((b + c) + n\mathbb{Z}) \\ &= (a + n\mathbb{Z}) + ((b + n\mathbb{Z}) + (c + n\mathbb{Z})) \end{aligned}$$

Zeigt die Assoziativität von $+$.

$$(a + n\mathbb{Z}) + (0 + n\mathbb{Z}) = ((a + 0) + n\mathbb{Z}) \overset{\mathbb{Z}\ Gruppe}{=} (a + n\mathbb{Z})$$

Zeigt, dass die Äquivalenzklasse von 0 das neutrale Element ist. Und

$$(a + n\mathbb{Z}) + ((-a) + n\mathbb{Z}) = ((a + (-a)) + n\mathbb{Z}) \overset{\mathbb{Z}\ Gruppe}{=} (0 + n\mathbb{Z})$$

zeigt, dass die Äquivalenzklasse vom Inversen von a in $\mathbb{Z}$ das Inverse der Äquivalenzklasse von a ist. Damit sind alle Gruppenaxiome erfüllt.
Da $\mathbb{Z}$ abelsch ist, ist auch $(\mathbb{Z}/n\mathbb{Z}, +, (0 + n\mathbb{Z}))$ abelsch.

(b) Sei ρ so eine Abbildung. Es muss gelten, dass wenn $(a+n\mathbb{Z}) = (b+n\mathbb{Z})$, dann auch $(a + d\mathbb{Z}) = (b + d\mathbb{Z})$. Nach Aufgabe 55(a) muss also die Implikation

$$n \mid (a - b) \Rightarrow d \mid (a - b) \tag{1}$$

gelten. Gilt umgekehrt die Implikation, so ist die Abbildung ρ wohldefiniert.
Gesucht sind also alle $d \in \mathbb{Z}$, sodass (1) gilt.

Behauptung: (1) $\Leftrightarrow d \mid n$

($\Rightarrow$)Gelte die Implikation, dann wähle $a = b + n$. Dann ist wegen (1)

$$n \mid (a - b) = n \Rightarrow d \mid n$$

die Aussage $d \mid n$ richtig, da $n \mid n$ immer wahr ist.

($\Leftarrow$)Umgekehrt sei $d \mid n$ richtig. Dann gilt wegen Lemma 87(a) auch die Implikation (1).

Addition:

$$\rho(((a+b)+n\mathbb{Z})) = ((a+b)+d\mathbb{Z}) = (a+d\mathbb{Z})+(b+d\mathbb{Z}) = \rho((a+n\mathbb{Z}))+\rho((b+n\mathbb{Z}))$$

Multiplikation:

$$\rho(((a \cdot b)+n\mathbb{Z})) = ((a \cdot b)+d\mathbb{Z}) = (a+d\mathbb{Z}) \cdot (b+d\mathbb{Z}) = \rho((a+n\mathbb{Z})) \cdot \rho((b+n\mathbb{Z}))$$

Beide Operationen vertragen sich mit ρ. Das bedeutet, dass ρ ein *Homomorphismus von Ringen* ist.

Behauptung: Sei $d \cdot s = n$. Dann ist

$$\rho^{-1}(\{(0 + d\mathbb{Z})\}) = \{(k \cdot d + n\mathbb{Z}) \mid k \in \{0, \ldots, s-1\}\}$$

Beweis:($\subseteq$) Sei $(a + n\mathbb{Z}) \in \rho^{-1}(\{(0 + d\mathbb{Z})\})$, also $\rho((a + n\mathbb{Z})) = (a + d\mathbb{Z}) = (0+d\mathbb{Z})$. Dann ist a ein Vielfaches von $d, a = t \cdot d$. t kann dargestellt werden als $t = qs + r$ für $r < s$. Wegen $a = t \cdot d = (qs + r) \cdot d = q \underbrace{sd}_{=n} + rd$ ist klar, dass $(a + n\mathbb{Z}) = (r \cdot d + n\mathbb{Z})$ und weil ist $r < s$ gilt ist $(a + n\mathbb{Z}) \in \{(k \cdot d + n\mathbb{Z}) \mid k \in \{0, \ldots, s-1\}\}$.

($\supseteq$)Sei $(k \cdot d + n\mathbb{Z})$ gegeben mit $k < s$. Dann ist $(k \cdot d + n\mathbb{Z})$ die k-fache Summe von $(d + n\mathbb{Z})$ mit sich selbst.

$$(k \cdot d + n\mathbb{Z}) = \sum_{j=1}^{k} (d + n\mathbb{Z})$$

Da ρ die Addition respektiert gilt:

$$\rho((k \cdot d + n\mathbb{Z})) = \rho(\sum_{j=1}^{k} (d + n\mathbb{Z})) = \sum_{j=1}^{k} \rho((d + n\mathbb{Z}))$$

$$= \sum_{j=1}^{k} (d + d\mathbb{Z}) = \sum_{j=1}^{k} (0 + d\mathbb{Z}) = (0 + d\mathbb{Z})$$

Somit gilt $(k \cdot d + n\mathbb{Z}) \in \rho^{-1}(\{(0 + d\mathbb{Z})\})$, was die Gleichheit zeigt.

Also ist $|\rho^{-1}(\{(0 + d\mathbb{Z})\})| = s$.

(c) Bezeichne $\mathcal{L}$ die Lösungsmenge der simultanen Kongruenz. Nutze die Gleichung

$$4 \cdot 7 - 3 \cdot 9 = 1$$

und definiere $e_1 := 4 \cdot 7 = 28$ und $e_2 := (-3) \cdot 9 = -27$. Dann ist

$$x := e_1 \cdot 2 + e_2 \cdot 3 = 28 \cdot 2 + (-27) \cdot 3 = -25$$

eine Lösung des Systems, wie man leicht nachprüfen kann.
Behauptung: $\mathcal{L} = ((-25) + 63\mathbb{Z})$
($\subseteq$) Sei $y \in \mathcal{L}$, dann gilt

$$y \equiv 2 \bmod 9$$

$$y \equiv 3 \bmod 7$$

Somit ist

$$y \equiv (-25) \bmod 9$$

$$y \equiv (-25) \bmod 7$$

Nach Aufgabe 55(a) ist also

$$9 \mid (y - (-25)) \wedge 7 \mid (y - (-25))$$

Da 7 und 9 teilerfremd sind ist

$$63 \mid (y - (-25))$$

wahr. Deshalb $y \in ((-25) + 63\mathbb{Z})$.
($\supseteq$) Sei $y \in ((-25) + 63\mathbb{Z})$. Dann ist

$$y \equiv (-25) \bmod 63 \Rightarrow y \equiv (-25) \bmod 9 \Rightarrow y \equiv 2 \bmod 9$$

$$y \equiv (-25) \bmod 63 \Rightarrow y \equiv (-25) \bmod 7 \Rightarrow y \equiv 3 \bmod 7$$

Also $y \in \mathcal{L}$. Dies zeigt die Gleichheit.