Lösungsskizzen zu Übung 4

Dominik Puhst

22. November 2012

Aufgabe 1c)

Gegeben waren die bekannte Äquivalenzrelation $\sim$ auf $\mathbb{N} \times \mathbb{N}$, definiert durch

$$(a, b) \sim (a', b') :\Leftrightarrow a + b' = a' + b,$$

die Addition auf $(\mathbb{N} \times \mathbb{N})/\sim$, definiert durch

$$[(a, b)] + [(c, d)] = [(a + c, b + d)]$$

sowie die Abbildung $\varphi : (\mathbb{N} \times \mathbb{N})/\sim \to \mathbb{Z}$, definiert durch

$$\varphi([(a, b)]) = a - b.$$

Wissend, dass die beiden φ-betreffenden Mengen mit ihrer entsprechenden Addition Gruppen bilden, sollte gezeigt werden, dass φ wohldefiniert und ein Gruppenisomorphismus ist.

Wohldefiniertheit

Seien $[(a, b)] = [(a', b')]$. Es ist zu zeigen, dass dann $\varphi([(a, b)]) = \varphi([(a', b')])$. Aus der Voraussetzung folgt, dass $(a, b) \sim (a', b')$, also dass gilt $a + b' = a' + b$. Dann ist $\varphi([(a, b)]) = a - b$ und $\varphi([(a', b')]) = a' - b'$. Wegen (in $\mathbb{Z}$) $a + b' = a' + b \Leftrightarrow a - b = a' - b'$ ist dies erfüllt.

Gruppenhomomorphismus

Es seien $[(a, b)], [(c, d)] \in (\mathbb{N} \times \mathbb{N})/\sim$. Dann gilt:

$$\begin{aligned}\varphi([(a, b)] + [(c, d)]) = \varphi([(a + c, b + d)]) = a + c - (b + d) = (a - b) + (c - d) \\ = \varphi([(a, b)]) + \varphi([(c, d)]),\end{aligned}$$

womit die Homomorphismuseigenschaft gezeigt ist.

Injektivität

Es ist zu zeigen, dass für $[(a,b)],[(c,d)] \in (\mathbb{N}\times\mathbb{N})/\sim$ gilt: $\varphi([(a,b)]) = \varphi([(c,d)]) \Rightarrow [(a,b)] = [(c,d)]$. Dies beweisen wir einfach durch Einsetzen der entpsrechenden Definitionen.

$$\begin{aligned}\varphi([(a,b)]) = \varphi([(c,d)]) &\Rightarrow a-b = c-d \Rightarrow a+d = c+b \\ &\Rightarrow (a,b)\sim(c,d) \Rightarrow [(a,b)] = [(c,d)]\end{aligned}$$

Surjektivität

Es ist zu zeigen, dass für jedes $z \in \mathbb{Z}$ ein $[(a,b)] \in (\mathbb{N}\times\mathbb{N})/\sim$ existiert, sodass $\varphi([(a,b)]) = z$ Dazu betrachten wir 3 Fälle (analog zu Aufgabenteil c der dritten Aufgabe von letzter Woche.

Fall 1: Sei $z = 0$, dann gilt $\varphi([(3,3)]) = 3-3 = 0$, also „wird 0 getroffen“.

Fall 2: Sei $z > 0$, dann gilt $\varphi([(z,0)]) = z - 0 = z$, also „werden postive ganze Zahlen getroffen“.

Fall 3: Sei $z < 0$, dann ist $-z \in \mathbb{N}$ und es gilt $\varphi([(0,-z)]) = 0-(-z) = z$, also „werden negative ganze Zahlen getroffen“.

Insgesamt ist die Abbildung also surjektiv und aus dem vorher gezeigten folgt, dass φ ein Gruppenisomorphismus ist.

Aufgabe 3

a) Zu zeigen ist, dass ein Körper stets Nullteilerfrei ist. Dies folgt bereits direkt aus der Abgeschlossenheit von $(K\setminus\{0\},\cdot)$. Zwei „Nichtnullen“ können also nicht zu „Null“ multipliziert werden.

b) Sei $m \in \mathbb{N}$ mit $m > 1$ und m *nicht prim*. Dann existieren Zahlen $p,q \in \mathbb{N}$ mit $1 < p,q < m$ und $m = p\cdot q$. Für $\mathbb{Z}_m$ bedeutet das

$$[p]\cdot[q] = [p\cdot q] = [m] = 0,$$

wobei $[p] \neq 0$ und $[q] \neq 0$ gilt. Demnach ist $\mathbb{Z}_m$ für m *nicht prim* nicht nullteilerfrei und kann somit nach a) kein Körper sein.

c) Zunächst müssen für feststellen, dass es genügt zu zeigen, dass in $\mathbb{Z}_p$, p *prim* zu jedem Element $a \in \mathbb{Z}_p\setminus\{[0]\}$ ein inverses Element $a^{-1} \in \mathbb{Z}_p\setminus\{[0]\}$ existiert, sodass $a\cdot a^{-1} = [1]$. Dies kann damit begründet werden, dass sich Eigenschaften wie Assoziativität, Kommutativität und so weiter aus dem rechnen in den ganzen Zahlen vererben, weiterhin das neutrale Element der Multiplikation in jedem $\mathbb{Z}_p$ enthalten ist etc, oder wir berufen uns auf die Vorlesung, in der gezeigt wurde, dass $(\mathbb{Z}_m,+,\cdot)$ ein

kommutativer Ring mit 1 ist und somit nur noch inverse zu einem Körper fehlen. Um nun zu zeigen, dass es diese inversen Elemente gibt, verwenden wir den Hinweis, der auf dem Aufgabenblatt stand und zeigen also zunächst, dass $\mathbb{Z}_p$, p *prim* nullteilerfrei ist.

Seien dazu also $[a], [b] \in \mathbb{Z}_p \setminus \{[0]\}$ mit $[a] \cdot [b] = [0]$. Dann existiert also ein $k \in \mathbb{Z}$, sodass $a \cdot b = k \cdot p$. Da in der Primfaktorzerlegung von $k \cdot p$ das p vorkommt, muss auch in der Primfaktorzerlegung von $a \cdot b$ ein p vorkommen. Dazu muss p allerdings in der Primfaktorzerlegung von a oder von b auftreten, was bedeuten würde, dass entweder a oder b Vielfache von p wären. Dann allerdings würde $[a] = [p] = [0]$ oder $[b] = [p] = [0]$ gelten, was der „Herkunft“ von $[a]$ und $[b]$ widerspricht. Demnach ist $\mathbb{Z}_p$, p *prim*, nullteilerfrei.

Nun sei $[a] \in \mathbb{Z}_p \setminus \{[0]\}$ beliebig, aber fest gewählt. Es bezeichne

$$f_a : \mathbb{Z}_p \setminus \{[0]\} \to \mathbb{Z}_p \setminus \{[0]\}$$

eine Abbildung, definiert durch

$$f_{[a]}([b]) = [a] \cdot [b].$$

Wir wollen zeigen, dass diese Abbildung injektiv ist. Seien dazu also die Bilder zweier Elemente $[b], [c] \in \mathbb{Z}_p \setminus \{[0]\}$ gleich, dann gilt:

$$\begin{aligned} f_{[a]}([b]) = f_{[a]}([c]) &\Rightarrow [a] \cdot [b] = [a] \cdot [c] \Rightarrow [a] \cdot [b] - [a] \cdot [c] = 0 \\ &\Rightarrow [a] \cdot ([b] - [c]) = 0 \Rightarrow [b] - [c] = 0 \Rightarrow [b] = [c] \end{aligned}$$

Dies ist genau das, was wir für Injektivität zeigen müssen. Wir haben dabei nur und in dieser Reihenfolge die Definition der Abbildung, die Existenz additiver inverser Elemente, das Distributivgesetz und die Nullteilerfreiheit verwendet.

Da Definitions- und Bildmenge von $f_{[a]}$ jeweils p Elemente haben (also endlich viele und gleich viele), folgt aus der Injektivität von $f_{[a]}$ sofort auch deren Surjektivität. Dies bedeutet insbesondere, dass auch die $[1]$ „getroffen wird“ und es deshalb zu $[a]$ ein inverses Element gibt. Da $[a]$ beliebig gewählt war, existieren inverse Elemente zu allen Elementen aus $\mathbb{Z}_p \setminus \{[0]\}$, womit $\mathbb{Z}_p$, mit p *prim*, tatsächlich ein Körper ist.