Übungsaufgaben zur Vorlesung Algebra und Zahlentheorie und ihre Didaktik Serie 2 Musterlösung

Dr. Daniel Skodlerack

6. Mai 2017

Aufgabe 1 (5+5 Punkte)**.** *Es seien n, m Elemente aus $\mathbb{N}_0$ und p ein Element aus $\mathbb{N}$. Zeigen Sie:*

1. *Aus $n \leq m \leq n^*$ folgt $m \in \{n, n^*\}$. Hinweis: Eine Induktion ist hier NICHT notwendig!*
2. *Die Ungleichung $pn < pm$ ist äquivalent zu $n < m$. Hinweis: Beweisen Sie zuerst die Rückrichtung.*

Lösung:

1. Beweis: Aus $n \leq m$ folgt nach der Kleiner-Gleich-Definition, dass ein $s \in \mathbb{N}_0$ existiert, so dass $m = n + s$ ist. Im Falle $s = 0$ gilt $n = m$ und im Falle $s \neq 0$ ist s nach Satz 2 ein Nachfolger eines Elementes t aus $\mathbb{N}_0$. Also gilt im zweiten Fall:

$$m = n + t^* \overset{Def.3b)}{=} (n + t)^* \overset{Lem.5}{=} n^* + t \overset{Def.}{\geq} n^*.$$

   Also gibt es kein Element, dass echt zwischen n und n^* liegt. q.e.d.

2. Beweis: Wir beweisen zuerst die Rückrichtung: Aus $n < m$ folgt nach Definition der Kleiner-Gleich-Relation und Satz 2, dass ein $t \in \mathbb{N}_0$ existiert, so dass $n + t^* = m$ gilt. Also gilt:

$$pn + p(t + 1) \overset{Distr.}{=} p(n + t^*) = pm.$$

   Beide Elemente p und $t + 1$ sind ungleich Null. Also ist das Produkt ungleich Null, nach der Nullteilerfreiheit aus der ersten Übung. Damit folgt $p(t + 1) \in \mathbb{N}$. Und somit $pn < pm$. Damit ist die Rückrichtung bewiesen.

   Wir haben drei Fälle für (n, m). Falls $n < m$, so folgt $pn < pm$, wie eben gezeigt. Falls $m < n$, dann folgt analog $pm < pn$, und im Fall $n = m$ folgt $pn = pm$. Mehr Fälle gibt es nicht für (n, m), da $(\mathbb{N}_0, \leq)$ totalgeordnet ist. Schaut man sich die drei Fälle an, sieht man, dass nur in einem der Fälle $pn < pm$ gelten kann, und zwar im Fall $n < m$. Damit ist die andere Richtung gezeigt. q.e.d.

Aufgabe 2 (5+5 Punkte)**.** *Zeigen Sie, dass die Teilbarkeitsrelation ($a|b \;\Leftrightarrow \exists : c \in \mathbb{Z} : b = ac$) auf der Menge der natürlichen Zahlen ($\mathbb{N} := \mathbb{N}_0 \setminus \{0\}$) eine Ordnungsrelation ist. Ist diese auch total? Beweisen Sie Ihre Antwort.*

Lösung: Vorbemerkung: Als erstes sei angemerkt, dass aus der ganzzahligen Gleichung $n = sm$ mit natürlichen Zahlen n und m folgt, dass s eine natürliche Zahl sein muss, denn aus $s = 0$ würde $n = 0$ und aus $s < 0$ würde nach 1.2 $-n = m(-s) > 0(-s) = 0$ folgen, und beides widerspräche $n > 0$.

1. Beweis: Reflexivität: Für $n \in \mathbb{N}$ gilt $1n = n$, und somit $n|n$. Transitivität: Aus $n|m$ und $m|l$ folgt nach Definition die Existenz von ganzen Zahlen s, t, so dass $m = sn$ und $l = tm$ gelten. Daraus folgt $l = stn$. Antisymmetrie: Wiederum nach Definition folgt aus $n|m|n$ die Existenz ganzer Zahlen s, t, so dass $n = sm$ und $m = tn$ gelten. Aus der Vorbemerkung wissen wir, dass s

und t natürliche Zahl sind, und aus Aufgabe 1.2 wissen wir, dass aus $s > 1$ die Ungleichung $n = ms > m = nt \geq n$ folgen würde. Also folgt mit Hilfe von Aufgabe 1.1 $s = 1$, und somit $n = m$. q.e.d.

2. Die Teilbarkeitsrelation auf $\mathbb{N}$ ist keine Totalordnung.

   Beweis: 1) Für zwei natürliche Zahlen n und m folgt aus $m|n$ die Ungleichung $m \leq n$, denn aus aus $n = ms$, $s \in \mathbb{N}$, folgt erstens nach 1.1 $s \geq 1$ und nach 1.2 $1m \leq sm = n$.

   3 teilt nicht 2, da $3 > 2$. Annahme $2|3$. Dann folgt $2|3 - 2 = 1$, woraus $0 < 2 \leq 1$ folgt. Also nach 1.1 folgt $1^* = 2 = 1$. Ein Widerspruch zu $1^* \neq 1$, siehe 1. Übung. Also sind 2 und 3 nicht mit $|$ vergleichbar, und somit ist $(\mathbb{N}, |)$ nicht total geordnet. q.e.d.

Aufgabe 3 (5+5 Punkte). *(Widerspruchsmethode des unendlichen Abstiegs)*

1. *Zeigen Sie, dass keine Abbildung $f : \mathbb{N}_0 \to \mathbb{N}_0$ existiert, die streng ordnungsumkehrend ist, d.h. die für alle $n, m \in \mathbb{N}_0$ mit $n < m$ die Ungleichung $f(n) > f(m)$ erfüllt.*

2. *Finden Sie alle ganzzahligen Lösungen der Gleichung $0 = X^3 + 7Y^3 + 49Z^3$.*

Lösung:

1. Beweis: Angenommen es gibt eine streng ordnungsumkehrende Abbildung $f : \mathbb{N}_0 \to \mathbb{N}_0$. Nach dem Wohlordnungssatz hat das Bild von f ein kleinstes Element $n = f(m)$. Also gilt $n \leq f(s)$ für alle $s \in \mathbb{N}_0$, insbesondere $f(m) = n \leq f(m+1)$. Ein Widerspruch dazu, dass f streng ordnungsumkehrend ist. q.e.d.

2. Als erstes hat die Gleichung die Lösung $(0, 0, 0)$. Angenommen es gäbe eine Lösung $(x, y, z) \neq (0, 0, 0)$. Wir zeigen, dass 7 alle Koordinaten teilt. Aus der Gleichung folgt $7|x^3$. Daraus folgt $7|x$: Beweis: Annahme x und 7 sind teilerfremd, so folgt aus dem Lemma von Bézout die Existenz einer ganzzahligen Linearkombination $a7 + bx = 1$. Also $1 = (a7 + bx)^3 = \tilde{a}7 + \tilde{b}x^3$, für geeignete ganzzahlige $\tilde{a}$ und $\tilde{b}$. Aus $7|x^3$ folgt nun mit der letzten Gleichung $7|1$. Ein Widerspruch. q.e.d.

   Aus $7|x$ folgt $7^3|x$, also $7|y^3$, mit der Gleichung, und somit $7|y$, woraus $7^3|y^3$ folgt. Und aus $7^3|x^3 + 7y^3 = 7^2z^3$ folgt $7|z^3$, also $7|z$. Damit teilt 7 alle Koordinaten. Wir schreiben $x = 7x_1$, $y = 7y_1$ und $z = 7z_1$. Folglich ist (x_1, y_1, z_1) eine Lösung der Gleichung aus der Aufgabe, und wir haben einen Widerspruch durch unendlichen Abstieg erlangt, da eine Lösung mit kleinerem Minimum der Beträge der nichtverschwindenden Koordinaten gefunden wurde. Genauer definiert man $f : \mathbb{N}_0 \to \mathbb{N}_0$ wie folgt: Man zeigt durch vollständige Induktion $7^n | \min\{|x|, |y|, |z|\}$, für alle $n \in \mathbb{N}_0$, etwa $\min\{|x|, |y|, |z|\} = 7^n t_n$, und definiert $f(n) := t_n$. Dann ist $f : \mathbb{N}_0 \to \mathbb{N}_0$ streng ordnungsumkehrend. Das ist ein Widerspruch zu Teil 1.

Aufgabe 4 (5+5* Punkte). *Wir bezeichnen zwei nichtleere Mengen M und N als bijektiv äquivalent, falls eine Bijektion von M nach N existiert.*

1. *Es sei T eine nichtleere endliche Teilmenge von $\mathbb{N}_0$. Zeigen Sie, dass eine natürliche Zahl m existiert, so dass T zu $\mathbb{N}^{\leq m}$ bijektiv äquivalent ist. Hinweis: Schauen Sie auf die Hinweise zu Satz 13.*

2.* *Es seien n und m natürliche Zahlen. Zeigen Sie, dass es genau dann eine Injektion von $\mathbb{N}^{\leq m}$ nach $\mathbb{N}^{\leq n}$ gibt, wenn $m \leq n$ gilt.*

Lösung:

1. Beweis: Wir beweisen die Aussage durch vollständige Induktion nach n, bezogen auf die folgende Familie von Aussagen:

   $A(n) :=$„Für jede nichtleere Menge T, zu der eine injektive Abbildung von T nach $\mathbb{N}^{\leq n}$ existiert, gibt es eine natürliche Zahl m, so dass T bijektiv äquivalent zu $\mathbb{N}^{\leq m}$ ist.“, $n \in \mathbb{N}$.

   (IA): $(n = 1)$: Es sei $\phi : T \to \mathbb{N}^{\leq 1}$ eine injektive Abbildung. Da das Bild von ϕ nichtleer ist und $\mathbb{N}^{\leq 1}$, nach Lemma 11, nur ein Element enhält, muss ϕ auch surjektiv sein.

(IS): $(n \to n+1)$: Es sei T eine nichtleere Menge und $\phi : T \to \mathbb{N}^{\leq n+1}$ eine injektive Abbildung. Falls $n+1$ nicht im Bild von ϕ liegt, dann können wir direkt die Induktionsvoraussetzung auf (T, ϕ) anwenden. Es sei also $n+1$ ein Element von $\phi(T)$. Dann gibt es ein $t_0 \in T$, so dass $\phi(t_0) = n+1$ ist. Also gibt es nach Induktionsvoraussetzung eine natürliche Zahl m, so dass $T \setminus \{t_0\}$ bijektiv äquivalent zu $\mathbb{N}^{\leq m}$ ist. Wähle eine Bijektion $\psi : T \setminus \{t_0\} \to \mathbb{N}^{\leq m}$. Wir setzen ψ auf T fort, indem wir t_0 auf $m+1$ abbilden. Also ist T bijektiv äquivalent zu $\mathbb{N}^{\leq m+1}$.

q.e.d.

2. Beweis: Wenn m kleiner gleich n ist, dann haben wir die Inklusion von $\mathbb{N}^{\leq m}$ nach $\mathbb{N}^{\leq n}$. Damit ist die Rückrichtung gezeigt.

   Zur Richtung „$\Rightarrow$“: Wir zeigen die Folge von Aussagen

   $$A(n) := „\forall_{m \in \mathbb{N}} : ((\exists_{\phi : \mathbb{N}^{\leq m} \to \mathbb{N}^{\leq n}} : \phi \text{ ist injekitv}) \Rightarrow m \leq n)“,\ n \in \mathbb{N}.$$

   (IA): $(n = 1)$: Es sei $\phi : \mathbb{N}^{\leq m} \to \mathbb{N}^{\leq 1}$ eine injektive Abbildung. Wenn m größer als 1 ist, dann können wir ϕ auf $\mathbb{N}^{\leq 2}$ einschränken. Da ϕ injektiv ist, gilt aber $\phi(1) \neq \phi(2)$. Also enthält $\mathbb{N}^{\leq 1}$ mindestens zwei verschiedene Elemente. Ein Widerspruch dazu, dass $\mathbb{N}^{\leq 1}$ nach Lemma 11 nur die 1 enthält.

   (IS): $(n \to n+1)$: Es sei $\phi : \mathbb{N}^{\leq m} \to \mathbb{N}^{\leq n+1}$ eine injektive Abbildung. Wenn $n+1$ nicht im Bild von ϕ liegt, dann können wir die Induktionsvoraussetzung anwenden und erhalten $m \leq n$. Wir brauchen also nur noch den Fall betrachten, dass $n+1$ im Bild von ϕ liegt, etwa $\phi(t_0) = n+1$. Wenn $m = 1$ ist, so ist $m \leq n$, und wir sind fertig. Also sei $m > 1$. Wir definieren $\tilde{\phi} : \mathbb{N}^{\leq m-1} \to \mathbb{N}^{\leq n}$ durch

   $$\tilde{\phi}(t) := \begin{cases} \phi(t), & \text{falls } t \neq t_0 \\ \phi(m), & \text{falls } t = t_0 \end{cases} .$$

   Diese Abbildung ist injektiv, weil ϕ injektiv ist. Also gilt nach Induktionsvoraussetzung $m - 1 \leq n$. Also gilt $m \leq n+1$. q.e.d.

$*$-Punkte sind Bonuspunkte.