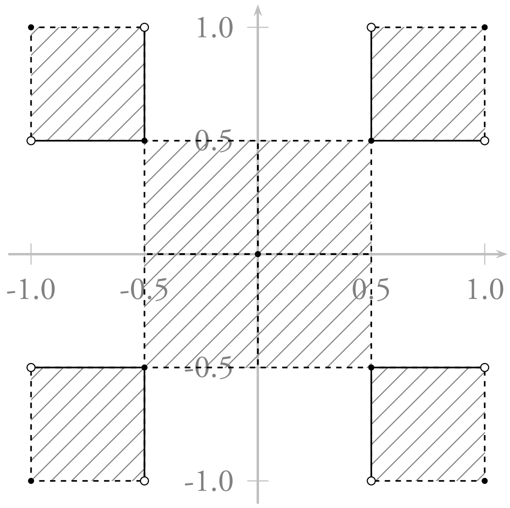
Mathematisches Institut der Universität München
Sommersemester 2014

Daniel Rost
Lukas-Fabian Moser

Grundlagen der Mathematik II
Lösungsvorschlag zum 5. Übungsblatt

Aufgabe 1. Man erhält die folgende Gestalt:



Aufgabe 2. Zunächst ist zu zeigen, daß $\preceq$ eine Ordnung, d.h. reflexiv, antisymmetrisch und transitiv ist. Dazu ist es hilfreich zu bemerken, daß aus $(x, y) \preceq (x', y')$ stets $x \leq x'$ folgt (denn nach Definition ist $(x, y) \preceq (x', y')$ nur dann wahr, wenn $x < x'$ oder $x = x'$ und eine weitere Bedingung erfüllt sind).

- *Reflexivität.* Ist $(x, y) \in \mathbb{N} \times \mathbb{N}$, so gilt $(x, y) \preceq (x, y)$, weil $x = x$ und $y \leq y$ ist, d.h. die zweite Hälfte der „oder"-Bedingung in der Definition von $\preceq$ ist erfüllt.

- *Antisymmetrie.* Es seien (x, y) und (x', y') in $\mathbb{N}\times\mathbb{N}$ mit $(x, y) \preceq (x', y')$ und gleichzeitig $(x', y') \preceq (x, y)$. Nach unserer Vorbemerkung oben folgt dann $x \leq x'$ und ebenso $x' \leq x$; also gilt $x = x'$. Nach Definition von $\preceq$ gilt dann aber sowohl $y \leq y'$ als auch $y' \leq y$, und dies bedeutet $y = y'$. Also ist insgesamt $(x, y) = (x', y')$.

- *Transitivität.* Es seien (x, y), (x', y') und (x'', y'') in $\mathbb{N} \times \mathbb{N}$ gegeben mit $(x, y) \preceq (x', y')$ und $(x', y') \preceq (x'', y'')$. Es ist zu beweisen, daß dann auch $(x, y) \preceq (x'', y'')$ ist. Nach unserer Vorbemerkung ist $x \leq x' \leq x''$. Ist sogar $x < x'$ oder $x' < x''$, so ist insgesamt $x < x''$, womit $(x, y) \preceq (x'', y'')$ automatisch erfüllt ist. Gilt aber keine dieser beiden strikten Ungleichungen, so ist $x = x'$ und $x' = x''$ und damit (nach Definition von $\preceq$) $y \leq y'$ sowie $y' \leq y''$. Insgesamt folgt dann $x = x''$ und $y \leq y''$, also $(x, y) \preceq (x'', y'')$.

Damit ist $\preceq$ tatsächlich eine Ordnung.

- Zum Nachweis, daß sie total ist, seien (x, y) und (x', y') in $\mathbb{N} \times \mathbb{N}$ beliebig vorgegeben. Gilt $x < x'$, so ist $(x, y) \preceq (x', y')$; gilt dagegen $x' < x$, so ist $(x', y') \preceq (x, y)$. Es bleibt also nur noch der Fall zu betrachten, daß keine dieser beiden Ungleichungen zutrifft; dann ist aber $x = x'$. Es trifft stets (mindestens) eine der Ungleichungen $y \leq y'$ und $y' \leq y$ zu; im ersten Fall gilt dann $(x, y) \preceq (x', y')$, im zweiten $(x', y') \preceq (x, y)$.

Der Name „lexikographische Ordnung" erklärt sich durch eine verbale Beschreibung der Definition von $\preceq$: Wir sortieren (x, y) dann vor (x', y') ein, wenn entweder $x \leq x'$ ist, oder wenn zwar $x = x'$ ist, jedoch $y < y'$. Man sortiert also änhand des ersten Eintrags" und dann „Paare mit gleichem ersten Eintrag anhand ihres zweiten Eintrags". Genauso sortiert man im Wörterbuch (Lexikographie ist die Wissenschaft vom Erstellen von Wörterbüchern): Nach dem Anfangsbuchstaben, und innerhalb einer Gruppe von Wörtern mit gleichem Anfangsbuchstaben nach dem zweiten Buchstaben. (Da die meisten Lexika aber aus Einträgen mit überwiegend mehr als nur zwei Buchstaben bestehen, wird das Sortierverfahren dort auf naheliegende Weise auf längere Buchstabenfolgen ausgedehnt: Stimmen von zwei Wörtern die ersten n Buchstaben überein, so wird ihre Reihenfolge anhand des $(n + 1)$-ten Buchstabens ermittelt.)

Aufgabe 3+4.

a) *Reflexivität.* Es gilt $(a, b) \sim (a, b)$ wegen $a + b = a + b$.

Symmetrie. Gilt $(a, b) \sim (c, d)$, also $a + d = b + c$, so ist auch $c + b = d + a$, also $(c, d) \sim (a, b)$.

Transitivität. Gilt $(a, b) \sim (c, d)$, also $a + d = b + c$, und $(c, d) \sim (e, f)$, also $c + f = d + e$, so folgt durch Addition beider Gleichungen $a + d + c + f = b + c + d + e$, also $a + f = b + e$, und das bedeutet $(a, b) \sim (e, f)$.

Der Beweis der Transitivät durch Addition zweier Gleichungen ist besonders leicht zu merken, aber man könnte ökonomischer vorgehen, indem man nur zur Gleichung $a + d = b + c$ auf beiden Seiten f addiert: Dann folgt nämlich

$$a + d + f = b + c + f = b + d + e,$$

also ebenfalls $a + f = b + e$. In jedem Fall jedoch benötigt man die „Kürzungsregel" in $\mathbb{N}$, die besagt, daß aus $a + x = b + x$ bereits $a = b$ folgt.

b) Es sei $[(a, b)] = [(a', b')]$, also $(a, b) \sim (a', b')$, und $[(c, d)] = [(c', d')]$, d.h. $(c, d) \sim (c', d')$. Zu beweisen ist, daß dann auch $(a + c, b + d) \sim (a' + c', b' + d')$ sowie $(ac + bd, ad + bc) \sim (a'c' + b'd', a'd' + b'c')$ gilt.

Die Voraussetzungen bedeuten $a + b' = b + a'$ sowie $c + d' = d + c'$. Damit gilt

$$(a + c) + (b' + d') = a + b' + c + d' = b + a' + d + c' = (b + d) + (a' + c'),$$

also $(a + c, b + d) \sim (a' + c', b' + d')$, womit die Wohldefiniertheit von „+" bewiesen ist.

Für „·" besteht ein stark vereinfachender Trick darin, den Austausch von (a, b) durch (a', b') und denjenigen von (c, d) durch (c', d') *getrennt* zu behandeln, also nachzuweisen, daß

$$\begin{array}{rl} \textbf{(I)} & (ac + bd, ad + bc) \sim (a'c + b'd, a'd + b'c) \\ \text{und} \quad \textbf{(II)} & (a'c + b'd, a'd + b'c) \sim (a'c' + b'd', a'd' + b'c') \end{array}$$

gilt (aufgrund der Transitivität von $\sim$ folgt dann das Gewünschte).[1] Es ist aber

$$\textbf{(I)} \qquad \begin{aligned} ac + bd + a'd + b'c &= (a + b')c + (b + a')d \\ &= (a' + b)c + (b' + a)d \\ &= a'c + b'd + ad + bc \end{aligned}$$

[1] Ein Indiz dafür, daß das die Argumentation tatsächlich vereinfachen könnte, besteht darin, daß der Beweis der Transitivität nicht „völlig trivial" war, man also in gewisser Weise schon „Arbeit investieren" mußte, die sich nun auszahlen kann. Unter Mathematikern sind heuristische Überlegungen dieser Art halb-humorvoll als „Gesetz von der Erhaltung der Schwierigkeit" bekannt.

sowie

$$\textbf{(II)} \qquad \begin{aligned} a'c + b'd + a'd' + b'c' &= a'(c + d') + b'(d + c') \\ &= a'(c' + d) + b'(d' + c) \\ &= a'c' + b'd' + a'd + b'c, \end{aligned}$$

womit beide Behauptungen bewiesen sind.

c)

(i) Nach Definition von „+“ ist $[(x, 0)] + [(y, 0)] = [(x + y, 0 + 0)] = [(x + y, 0)]$.

(ii) Nach Definition von „·“ ist $[(x, 0)] \cdot [(y, 0)] = [(x \cdot y + 0 \cdot 0, x \cdot 0 + 0 \cdot y)] = [(xy, 0)]$.

(iii) Ist $[(x, 0)] = [(y, 0)]$, also $(x, 0) \sim (y, 0)$, so bedeutet das definitionsgemäß $x + 0 = 0 + y$, also $x = y$.

d) Um zu zeigen, daß $(Z, +, \cdot)$ ein kommutativer Ring ist, ist zu überprüfen, daß $+$ und $\cdot$ assoziative und kommutative Verknüpfungen sind, die ein neutrales Element besitzen; ferner, daß bezüglich $+$ inverse Elemente existieren, und daß zwischen $+$ und $\cdot$ das Distributivgesetz gilt.

Ans Werk:

- **Assoziativität von $+$ und $\cdot$**
  Für $[(a, b)]$, $[(c, d)]$ und $[(e, f)]$ gilt

$$\begin{aligned} ([(a, b)] + [(c, d)]) + [(e, f)] &= [(a + c, b + d)] + [(e, f)] = [(a + c + e, b + d + f)] \\ &= [(a, b)] + [(c + e, d + f)] = [(a, b)] + ([(c, d)] + [(e, f)]), \end{aligned}$$

  was die Assoziativität von $+$ beweist. Für die Multiplikation rechnen wir

$$\begin{aligned} ([(a, b)] \cdot [(c, d)]) \cdot [(e, f)] &= [(ac + bd, ad + bc)] \cdot [(e, f)] \\ &= [((ac + bd)e + (ad + bc)f, (ac + bd)f + (ad + bc)e)] \\ &= [(ace + bde + adf + bcf, acf + bdf + ade + bce)] \end{aligned}$$

  und

$$\begin{aligned} [(a, b)] \cdot ([(c, d)] \cdot [(e, f)]) &= [(a, b)] \cdot [(ce + df, cf + de)] \\ &= [(a(ce + df) + b(cf + de), a(cf + de) + b(ce + df))] \\ &= [(ace + adf + bcf + bde, acf + ade + bce + bdf)], \end{aligned}$$

  und die letzten beiden Ergebnisse stimmen überein, womit die Assoziativität von $\cdot$ bewiesen ist.

- **Kommutativität**
  Für $[(a, b)]$ und $[(c, d)]$ gilt

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

  so daß $+$ kommutativ ist, sowie

$$[(a, b)] \cdot [(c, d)] = [(ac + bd, ad + bc)] = [(ca + db, cb + da)] = [(c, d)] \cdot [(a, b)],$$

  so daß $\cdot$ kommutativ ist.

- **Neutrale Elemente**

  Ich behaupte, daß $[(0,0)]$ neutrales Element für $+$ und $[(1,0)]$ neutrales Element für $\cdot$ ist. Aufgrund der Kommutativität ist das jeweils nur einseitig zu überprüfen; die Rechnung lautet:

  $$[(0,0)] + [(a,b)] = [(0+a, 0+b)] = [(a,b)]$$

  sowie

  $$[(1,0)] + [(a,b)] = [(1 \cdot a + 0 \cdot b, 1 \cdot b + 0 \cdot a)] = [(a,b)].$$

- **Inverse Elemente bezüglich** $+$

  Ich behaupte, daß zum Element $[(a,b)]$ ein inverses Element bezüglich $+$ existiert, nämlich $[(b,a)]$. Denn es ist

  $$[(a,b)] + [(b,a)] = [(a+b, a+b)] = [(0,0)],$$

  denn allgemein ist $[(x,x)] = [(0,0)]$ für alle $x \in \mathbb{N}_0$ wegen $x+0 = x+0$, also $(x,x) \sim (0,0)$.

- **Distributivgesetz**

  Aufgrund der Kommutativität genügt wieder eine einzige Form von Distributivität: Es ist zu beweisen, daß

  $$[(a,b)] \cdot ([(c,d)] + [(e,f)]) = ([(a,b) \cdot [(c,d)]) + ([(a,b) \cdot [(e,f)])$$

  gilt. Die linke Seite ergibt

  $$\begin{aligned} [(a,b)] \cdot [(c+e, d+f)] &= [a(c+e) + b(d+f), a(d+f) + b(c+e)] \\ &= [ac + ae + bd + bf, ad + af + bc + be], \end{aligned}$$

  die rechte Seite

  $$[(ac+bd, ad+bc)] + [(ae+bf, af+be)] = [(ac+bd+ae+bf, ad+bc+af+be)],$$

  und da beide Ergebnisse übereinstimmen, ist damit die Distributivität bewiesen.

e) Es sei $[(a,b)] \in Z$ gegeben. Dann gibt es drei Möglichkeiten:

- Ist $a = b$, so ist $[(a,b)] = [(0,0)] = 0$, wie bereits bei der Diskussion der inversen Elemente bezüglich $+$ gezeigt.
- Ist $a > b$, so finden wir ein $x \in \mathbb{N}$ mit $a = b + x$. Dann ist aber $[(a,b)] = [(b+x, b)] = [(x,0)]$ wegen $b + x + 0 = b + x$, und dieses Element ist einfach $x \in \mathbb{N}$ (wir fassen ja $\mathbb{N}$ als Teilmenge von Z auf).
- Ist $a < b$, so finden wir ein $x \in \mathbb{N}$ mit $b = a + x$, und dann ist $[(a,b)] = [(a, a+x)] = [(0,x)] = -[(x,0)] = -x$.

Es tritt also tatsächlich stets eine der drei angegebenen Möglichkeiten ein. (Die Eindeutigkeitsaussagen in (ii) und (iii) folgen dabei aus Teilaufgabe c) (iii).)