Universität Konstanz
Fachbereich Mathematik und Statistik
Sommersemester 2011

Christoph Hanselka
Aaron Kunert
Markus Schweighofer

Lösungsblatt 1 zur Zahlentheorie

Aufgabe 1.

(a) Seien $A,B \in S$. Wir zeigen zunächst, dass die Summe wohldefiniert also endlich ist. Seien dazu $i,k \in \mathbb{N}$ fixiert. Dann gibt es ein $r \in \mathbb{N}$, so dass $A(i,j) = 0$ für alle $j \geq r$. Daher ist

$$AB(i,k) = \sum_{j \in \mathbb{N}} A(i,j)B(j,k) = \sum_{j \leq r} A(i,j)B(j,k)$$

und die Multiplikation ist wohldefiniert. Als nächstes zeigen wir $AB \in S$. Dazu genügt es zu zeigen, dass jede Spalte und jede Zeile von AB endlichen Träger hat. Sei $i \in \mathbb{N}$ fixiert. Dann gibt es nur endlich viele $j \in \mathbb{N}$ mit $A(i,j) \neq 0$. Insbesondere gibt es ein $s \in \mathbb{N}$, so dass $B(j,t) = 0$ für alle $t \geq s$ und für alle $j \in \mathbb{N}$ mit $A(i,j) \neq 0$ ist. Daher ist auch

$$AB(i,t) = \sum_{j \in \mathbb{N}} A(i,j)B(j,t) = 0$$

für alle $t \geq s$. Dies zeigt, dass alle Zeilen von AB endlichen Träger haben. Analog zeigt man, dass alle Spalten von AB endlichen Träger haben.

(b) Seien $A,B,C \in S$. Für $i,l \in \mathbb{N}$ ist

$$\begin{aligned}
((AB)C)(i,l) &= \sum_{k \in \mathbb{N}} (AB)(i,k)C(k,l) \\
&= \sum_{k \in \mathbb{N}} \left(\sum_{j \in \mathbb{N}} A(i,j)B(j,k) \right) C(k,l) \\
&= \sum_{k \in \mathbb{N}} \sum_{j \in \mathbb{N}} (A(i,j)B(j,k))C(k,l) \\
&= \sum_{k \in \mathbb{N}} \sum_{j \in \mathbb{N}} A(i,j)(B(j,k)C(k,l)) \\
&= \sum_{j \in \mathbb{N}} \sum_{k \in \mathbb{N}} A(i,j)(B(j,k)C(k,l)) \\
&= \sum_{j \in \mathbb{N}} A(i,j) \left(\sum_{k \in \mathbb{N}} B(j,k)C(k,l) \right) \\
&= \sum_{j \in \mathbb{N}} A(i,j)(BC)(j,l)) \\
&= A(BC)(i,l).
\end{aligned}$$

Dabei sei bemerkt, dass alle auftretenden Summen endlich und daher obige Umformungen gerechtfertigt sind. Dies zeigt die Assoziativität der Multiplikation. Weiter zeigt man

$$\begin{aligned}((A+B)C)(i,l) &= \sum_{k\in\mathbb{N}}(A+B)(i,k)C(k,l)\\ &= \sum_{k\in\mathbb{N}}(A(i,k)+B(i,k))C(k,l)\\ &= \sum_{k\in\mathbb{N}}(A(i,k)C(k,l)+B(i,k)C(k,l))\\ &= \sum_{k\in\mathbb{N}}A(i,k)C(k,l)+\sum_{k\in\mathbb{N}}B(i,k)C(k,l)\\ &= (AC)(i,l)+BC(i,l).\end{aligned}$$

Dies zeigt die Distrubutivität von Addition und Multiplikation. Wir definieren $E \in R^{\mathbb{N}\times\mathbb{N}}$ durch

$$E(i,k) = \begin{cases}1 & \text{für } i=k\\ 0 & \text{für } i\neq k\end{cases}.$$

Da in jeder Spalte und jeder Zeile von E nur ein Element verschieden von 0 ist, gilt $E \in S$. Weiter ist

$$\begin{aligned}(AE)(i,k) &= \sum_{j\in\mathbb{N}}A(i,j)E(j,k)\\ &= A(i,k)\\ &= (EA)(i,k).\end{aligned}$$

Dies zeigt, dass S ein Ring mit dem Einselement E ist.

(c) Für $A \in S$ und $i,j \in \mathbb{N}$ ist $A_1(i,j) = A(i,2j-1)$ und $A_2(i,j) = A(i,2j)$. Dies zeigt, dass $A_1,A_2 \in S$ und damit f wohldefiniert ist. Wir zeigen, dass die Abbildung $f_1\colon A \mapsto A_1$ ein S–Modulhomomorphismus ist. Seien dazu $A,B \in S$. Es ist

$$\begin{aligned}f_1(A+B)(i,j) &= (A+B)(i,2j-1)\\ &= A(i,2j-1)+B(i,2j-1)\\ &= (f_1(A)+f_1(B))(i,j).\end{aligned}$$

Weiter ist

$$\begin{aligned}f_1(AB)(i,j) &= (AB)(i,2j-1)\\ &= \sum_{k\in\mathbb{N}}A(i,k)B(k,2j-1)\\ &= (Af_1(B))(i,j),\end{aligned}$$

was zeigt, dass f_1 ein S–Modulhomomorphismus ist. Analog zeigt man, dass auch auch f_2 und damit f ein S–Modulhomomorphismus ist. Wir definieren die Abbildung

$$\begin{aligned}g\colon S^2 &\to S\\ (A,B) &\longmapsto g(A,B),\end{aligned}$$

mit

$$g(A,B)(i,j) = \begin{cases}A(i,\frac{j}{2}) & \text{falls } j \text{ gerade}\\ B(i,\frac{j+1}{2}) & \text{falls } j \text{ ungerade}\end{cases}.$$

Man rechnet leicht nach, dass $f\circ g = \mathrm{id}_{S^2}$ und $g\circ f = \mathrm{id}_S$ gilt. Daher ist f bijektiv uns somit ein S–Modulisomorphismus.

Aufgabe 2.
Sei R ein Ring, $f\colon M \longrightarrow N$ ein R–Modulhomomorphismus und U ein Untermodul von M mit $U \subseteq \ker(f)$. Sei weiter $\pi\colon M \longrightarrow M/U$ der natürliche Epimorphismus. Zu zeigen ist, dass genau ein R–Modulhomomorphismus $\overline{f}\colon M/U \longrightarrow N$ existiert, so dass das Diagramm

$$\begin{tikzcd} M \arrow[rr, "f"] \arrow[dr, "\pi"'] & & N \\ & M/U \arrow[ur, "\overline{f}"'] & \end{tikzcd}$$

kommutiert. Dazu definieren wir die Abbildung $\overline{f}$ für $\overline{v} \in M/U$ durch $\overline{f}(\overline{v}) := f(v)$. Da eine Nebenklasse $\overline{v}$ im Allgemeinen durch mehrere Elemente aus M repräsentiert wird, ist zunächst zu überprüfen, dass diese Definition nicht vom Vertreter abhängt. Seien also $w,v \in M$ mit $\overline{v} = \overline{w}$. Dann ist $f(v) - f(w) = f(w - v) = 0$, denn $w - v \in U \subseteq \ker(f)$. Daher ist insbesondere $f(v) = f(w)$ und die Abbildung $\overline{f}$ ist wohldefiniert. Nun überprüft man, dass es sich bei $\overline{f}$ um einen R–Modulhomomorphismus handelt. Sei dazu $\overline{v},\overline{w} \in M/U$ und $r \in R$. Es ist $\overline{f}(\overline{v}+\overline{w}) = \overline{f}(\overline{v + w}) = f(v + w) = f(v) + f(w) = \overline{f}(\overline{v}) + \overline{f}(\overline{w})$ und weiter $\overline{f}(r\overline{v}) = \overline{f}(\overline{rv}) = f(rv) = rf(v) = r\overline{f}(\overline{v})$, was zeigt, dass $\overline{f}$ in der Tat ein Homomorphismus ist. Offenbar ist auch $(\overline{f} \circ \pi)(v) = \overline{f}(\overline{v}) = f(v)$ für alle $v \in M$, was zeigt, dass obiges Diagramm kommutiert. Angenommen es gäbe noch eine weitere Abbildung $g\colon M/U \longrightarrow N$, die obiges Diagramm kommutativ macht. Dann müsste gelten $g \circ \pi = f$ und daher $g(\overline{v}) = f(v)$ für alle $v \in M$. Dann ist aber offensichtlich $g = \overline{f}$.

Zusatz: Ist $U = \ker(f)$, so ist $\overline{f}$ ein Isomorphismus auf das Bild von f.
Aus der Konstruktion von $\overline{f}$ folgt sofort, dass $\mathrm{im}(f) = \mathrm{im}(\overline{f})$ gilt. Es bleibt also zu zeigen, dass $\overline{f}$ injektiv ist. Angenommen $\overline{f}(\overline{v}) = 0$ für ein $v \in M$, so ist $f(v) = 0$ und daher $v \in \ker(f)$. Insbesondere haben wir $\overline{v} = 0$, was die Injektivität von f zeigt.

Aufgabe 3.
Typische Fragen wären beispielsweise gewesen, warum ein R–Modul im Allgemeinen keine Basis besitzt, oder warum in einem R–Modul M die Situation $rv = 0$ mit $r \in \mathbb{R} \setminus \{0\}$ und $v \in M \setminus \{0\}$ auftreten kann.