**Universität Konstanz**
**Fachbereich Mathematik und Statistik**
**Sommersemester 2011**

Christoph Hanselka
Aaron Kunert
Markus Schweighofer

# Lösungsblatt 2 zur Zahlentheorie

**Aufgabe 1.**

(a) Der Kern von $f$ ist gerade das Bild der Nullabbildung. Daher ist $\ker f = (0)$ und $f$ ist injektiv. Weiter ist das Bild von $g$ gerade der Kern der Nullabbildung. Daher ist $\mathrm{im}(g) = N$ und somit ist $g$ surjektiv.

(b) Wir verwenden den Isomorphiesatz: Es ist $M/\ker(g) \cong \mathrm{im}(g)$. Wir hatten schon gesehen, dass $g$ surjektiv ist, daher ist $\mathrm{im}(g) = N$. Weiter ist $\ker(g) = \mathrm{im}(f) = f(L)$. Daraus folgt $M/f(L) \cong N$.

(c) Wir zeigen beide Richtungen:
(i) $\Rightarrow$ (ii):
Sei $i\colon M \longrightarrow L$ mit $i \circ f = \mathrm{id}_L$. Der erste Schritt ist, dass wir uns zu $x \in N$ ein ausgezeichnetes Urbild von $x$ unter $g$ konstruieren. Seien $y_1$,$y_2 \in M$ mit $g(y_1) = g(y_2) = x$. Behauptung: Das Element $y_1 - (f \circ i)(y_1)$ ist ein Urbild von $x$ und es gilt $y_1 - (f \circ i)(y_1) = y_2 - (f \circ i)(y_2)$. Der erste Teil der Behauptung folgt sofort aus $g \circ f = 0$. Da sowohl $y_1 - (f \circ i)(y_1)$ als auch $y_2 - (f \circ i)(y_2)$ von $g$ auf $x$ abgebildet werden, liegt ihre Differenz $z := (y_1 - y_2) - (f \circ i)(y_1 - y_2)$ in $\ker(g) = \mathrm{im}(f)$. Anderseits ist $z \in \ker(i)$, denn es ist $i(z) = i(y_1 - y_2) - (i \circ f \circ i)(y_1 - y_2) = i(y_1 - y_2) - (\mathrm{id}_L \circ i)(y_1 - y_2) = i(y_1 - y_2) - i(y_1 - y_2) = 0$. Also ist $z \in \mathrm{im}(f) \cap \ker(i)$. Wegen $z \in \mathrm{im}(f)$ existiert ein $t \in L$ mit $z = f(t)$. Wegen $z \in \ker(i)$ folgt $0 = i(z) = (i \circ f)(t) = t$ daher ist $z = f(0) = 0$. Insbesondere ist $y_1 - y_2 - (f \circ i)(y_1 - y_2) = 0$. Da $g$ surjektiv ist, ist somit die Abbildung $j\colon N \longrightarrow M$ mit $x \mapsto y - (f \circ i)y$ für ein $y \in g^{-1}(x)$ wohldefiniert. Nach Konstruktion ist $g \circ j = \mathrm{id}_N$. Bleibt nur noch zu zeigen, dass $j$ ein $R$–Modulhomomorphismus ist. Sei dazu $x_1$,$x_2 \in N$ und $r \in R$. Seien $y_1$,$y_2 \in M$ mit $g(y_1) = x_1$ und $g(y_2) = x_2$. Dann ist $j(rx) = ry - (f \circ i)(ry) = r(y - (f \circ i)(y)) = rj(x)$, denn $ry$ ist ein Urbild von $rx$ unter $g$. Weiter ist $j(x_1 + x_2) = (y_1 + y_2) - (f \circ i)(y_1 + y_2) = y_1 - (f \circ i)(y_1) + y_2 - (f \circ i)(y_2) = j(x_1) + j(x_2)$, denn $y_1 + y_2$ ist ein Urbild von $x_1 + x_2$ unter $g$.
(ii) $\Rightarrow$ (i):
Sei $j\colon N \longrightarrow M$ mit $g \circ j = \mathrm{id}_N$. Da $f$ injektiv ist, ist die Abbildung $h\colon L \longrightarrow \mathrm{im}(f) = \ker(g)$ mit $h(x) = f(x)$ ein Isomorphismus. Wir definieren $i_0 := h^{-1}\colon \mathrm{im}(f) \longrightarrow L$. Sei $m \in M$, dann definieren wir $i\colon M \longrightarrow L$ durch $i(m) := i_0(m - (j \circ g)(m))$. Man beachte dass $g(m) - g((j \circ g)(m)) = g(m) - (g \circ j \circ g)(m) = g(m) - g(m) = 0$ gilt und daher $m - (j \circ g)(m) \in \ker(g) = \mathrm{im}(f)$ ist. Insbesondere ist die Abbildung $i$ wohldefiniert. Weiter ist $i = i_0 \circ (\mathrm{id}_M - (j \circ g))$ und daher ebenfalls ein $R$–Modulhomomorphismus, da Summen und Verkettungen von $R$–Modulhomomorphismen wieder ebensolche sind. Schließlich ist noch zu zeigen, dass $f \circ i = \mathrm{id}_L$ ist. Sei dazu $x \in L$. Dann ist $(i \circ f)(x) = i_0(f(x) - (j \circ g)(f(x))) = (i_0)(f(x)) = x$.

**Bemerkung:**
In der Vorlesung wurde gezeigt, dass ein idempotentes Element $e \in \mathrm{End}(M)$ eine Zerlegung von $M$ induziert, denn es gilt $M = e(M) \oplus (1 - e)(M)$. Existiert nun ein $i\colon M \longrightarrow L$ mit $i \circ f = \mathrm{id}_L$, so ist $(f \circ i)^2 = f \circ i \circ f \circ i = f \circ \mathrm{id}_L \circ i = f \circ i$. Daher ist $e := f \circ i \in \mathrm{End}(M)$ idempotent. Weiter lässt sich leicht nachrechnen, dass $g \circ (1 - e) = g$ ist. Insbesondere ist $g$ eingeschränkt auf den direkten Summanden $(1 - e)(M)$ surjektiv. Analog wie im Beweis oben, lässt sich auch zeigen, dass $g$ eingeschränkt auf $(1 - e)(M)$ injektiv ist. Dann folgt auch sofort die Existenz eines $j\colon N \longrightarrow M$ mit $g \circ j = \mathrm{id}_N$. Analog lässt sich die andere Richtung zeigen. Dies gibt einen etwas konzeptionelleren Zugang zu dieser Aufgabe.

(d) Sei $j\colon N \longrightarrow M$ mit $g \circ j = \mathrm{id}_N$ und $m \in M$. Dann ist $m = (m-(j\circ g)(m))+(j\circ g)(m)$. Dabei hatten wir schon gesehen, dass $m-(g\circ j)(m) \in \ker(g)$ ist. Also ist lässt sich jedes $m \in M$ schreiben als Summe eines Elements aus $\ker(g)$ und eines Elements aus $\mathrm{im}(j)$. Es ist also $M = \ker(g)+\mathrm{im}(j)$. Wir zeigen nun, dass diese Summe direkt ist. Sei dazu $x \in \ker(g)\cap\mathrm{im}(j)$. Wegen $x \in \mathrm{im}(j)$ gibt es ein $y \in N$ mit $x = j(y)$. Wegen $x \in \ker(g)$ folgt $0 = g(x) = (g\circ j)(y) = y$. Also ist $x = j(y) = j(0) = 0$. Insbesondere ist $M = \ker(g) \oplus \mathrm{im}(j)$. Da $f$ injektiv ist und $\mathrm{im}(f) = \ker(g)$ ist, gilt $\ker(g) \cong L$. Auf der anderen Seite ist $g \circ j = \mathrm{id}_N$ und daher ist auch $j$ injektiv, woraus $\mathrm{im}(j) \cong N$ folgt. Zusammengenommen ist also $M = \ker(g) \oplus \mathrm{im}(j) \cong L \oplus N$.

**Aufgabe 2.**
Wir schreiben $j\colon M \longrightarrow M+N, x \mapsto x$ für die Einbettungsabbildung von $M$ in $M+N$. Weiter schreiben wir $\pi\colon M+N \longrightarrow (M+N)/N$ für den natürlichen Epimorphismus. Sei $f := \pi \circ j$. Behauptung: $f$ ist surjektiv. Sei dazu $\overline{x} \in (M+N)/N$. Wegen $x \in M+N$ gibt es $m \in M$ und $n \in N$ mit $x = m+n$. Dann ist $\overline{x} = \pi(m+n) = \pi(m)+\pi(n) = \pi(m)$, denn $\pi(n) = 0$. Daher ist $\overline{x} = \pi(m) = f(m)$, was zeigt, dass $f$ surjektiv ist. Als nächstes betrachten wir den Kern von $f$. Es ist

$$\begin{aligned} x \in \ker(f) &\Leftrightarrow (\pi\circ j)(x) = 0 \\ &\Leftrightarrow j(x) \in \ker(\pi) \\ &\Leftrightarrow j(x) \in N \\ &\Leftrightarrow x \in N \cap M. \end{aligned}$$

Nun verwendet man den Isomorohiesatz und erhält

$$(N+M)/N \cong M/\ker(f) \cong M/(M\cap N).$$

**Aufgabe 3.**
Zunächst zeigt man, dass $L$ ein Untermodul von $\mathbb{Z}^3$ ist. Offensichtlich ist $0 = (0,0,0) \in L$. Seien $(x_1,y_1,z_1),(x_2,y_2,z_2) \in L$. Dann ist

$$(x_1+x_2)+2(y_1+y_2)+3(z_1+z_2) = (x_1+2y_1+3z_1)+(x_2+2y_2+3z_2) = 0+0 = 0.$$

Analog zeigt man, dass $(x_1+x_2,y_1+y_2,z_1+z_2)$ die zweite Gleichung erfüllt. Sei weiter $k \in \mathbb{Z}$ und $v = (x,y,z) \in L$. Dann ist

$$kx+2ky+3kz = k(x+2y+3z) = 0.$$

Ebenso erfüllt $kv$ die zweite Gleichung und wir haben gezeigt, dass $L$ ein Untermodul von $\mathbb{Z}^3$ ist. Die beiden Gleichungen in der Definition von $L$ lassen sich als Lösungsmenge eines linearen Gleichungssystem über $\mathbb{Z}$ darstellen. Die Lösungsmenge in $\mathbb{Z}^3$ bleibt unverändert, wenn man Zeilen vertauscht oder ein ganzzahliges Vielfaches einer Zeile zu einer anderen Zeile hinzuaddiert. Daher ist $L$ die genaue Lösungsmenge der Systeme

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 4 & 9 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 6 \end{pmatrix} \text{ und } \begin{pmatrix} 1 & 0 & -3 \\ 0 & 2 & 6 \end{pmatrix}.$$

Die Gleichung $2y-6z = 0$ ist genau dann erfüllt, wenn $y = -3z$ ist. Die Gleichung $x-3z$ genau dann, wenn $x = 3z$ ist. Daher sind alle Lösungen von der Form $(3k,-3k,k) = k(3,-3,1)$ für $k \in \mathbb{Z}$. Also ist $L = \mathbb{Z}(3,-3,1)$. Dies zeigt, dass $L$ frei ist. Die Basen von $L$ sind $\{(3,-3,1))\}$ und $\{(-3,3,-1)\}$. Behauptung: Dies sind alle Basen von $L$. In der Vorlesung wurde gezeigt, dass Basen von freien Moduln endlichem Rangs über einem kommutativen Ring stets die gleiche Anzahl an Elementen besitzen. Angenommen es gäbe noch eine weitere Basis, so müsste diese aus genau einem Element $v$ bestehen. Weiter ist $v$ von der Form $(3k,-3k,k)$ und es müsste ein $l \in \mathbb{Z}$ geben, so dass $lv = (3,-3,1)$ ist. Betrachtet man nur die dritte Komponente, so müsste insbesondere $kl = 1$ sein, was zeigt, dass $k \in \{-1,1\}$ sein muss.