Universität Konstanz
Fachbereich Mathematik und Statistik
Sommersemester 2011

Christoph Hanselka
Aaron Kunert
Markus Schweighofer

Lösungsblatt 4 zur Zahlentheorie

Aufgabe 1.
Ist R ein Körper, so ist jeder R–Modul ein R–Vektorraum und somit frei. Sei nun umgekehrt jeder endlich erzeugte R–Modul frei. Wegen $1 \neq 0$ gibt es ein maximales Ideal $\mathfrak{m}$ in R. Der R–Modul $R/\mathfrak{m}$ ist endlich erzeugt und nach Voraussetzung frei. Daher gibt es ein $n \in \mathbb{N}$ und einen Isomorphismus $f\colon R^n \xrightarrow{\sim} R/\mathfrak{m}$. Sei $i\colon R \hookrightarrow R^n$ eine Einbettung. Dann ist $\varphi := f \circ i\colon R \longrightarrow R/\mathfrak{m}$ injektiv. Ist $x \in \mathfrak{m}$ so ist $\varphi(x) = \varphi(x \cdot 1) = \overline{x\varphi(1)} = 0$. Daher ist $\mathfrak{m} = 0$ und somit ist $R = R/\mathfrak{m}$ ein Körper.

Aufgabe 2.

(a) Sei $I \subseteq R$ ein Ideal in einem Integritätsring R. Angenommen $I = I_1 \oplus I_2$ als R–Moduln mit $I_1, I_2 \neq (0)$. Sei $0 \neq x \in I_1$ und $0 \neq y \in I_2$. Dann ist $xy \in I_1 \cap I_2 = (0)$. Dies ist ein Widerspruch, da R nullteilerfrei ist.

(b) Wir definieren $f\colon I_1 \cap I_2 \longrightarrow I_1 \oplus I_2$ als $f(x) = (x, -x)$ offensichtlich ist f ein injektiver R–Modulhomomorphismus. Weiter setzen wir $g\colon I_1 \oplus I_2 \longrightarrow R$ mit $g(x,y) = x + y$. Da I_1 und I_2 koprime Ideale sind, ist die Abbildung g surjektiv. Es ist

$$\begin{aligned}
(x,y) \in \ker(g) &\Leftrightarrow x + y = 0\\
&\Leftrightarrow x = -y\\
&\Leftrightarrow x \in I_1 \cap I_2 \text{ und } y = -x\\
&\Leftrightarrow (x,y) = (x, -x) \text{ für ein } x \in I_1 \cap I_2\\
&\Leftrightarrow (x,y) \in \operatorname{im}(f).
\end{aligned}$$

Dies zeigt, dass die Sequenz

$$0 \longrightarrow I_1 \cap I_2 \xrightarrow{f} I_1 \oplus I_2 \xrightarrow{g} R \longrightarrow 0$$

exakt ist.

(c) Wir bemerken, dass R ein freier R–Modul ist und daher zerfällt obige kurze exakte Sequenz (vgl. Aufgabe 3 auf Blatt 3). Insbesondere ist dann $I_1 \oplus I_2 \cong R \oplus (I_1 \cap I_2)$ als R–Moduln (vgl. Aufgabe 1.(d) auf Blatt 2). Die Ideale I_1, I_2, R und $I_1 \cap I_2$ sind jeweils unzerlegbare R–Moduln, da R als nullteilerfrei vorausgesetzt wurde.

(d) Wir setzen $R = \mathbb{Z}[X]$ und definieren die Ideale (bzw. Moduln) $I_1 := (2,X)$ und $I_2 := (3,X)$. Wegen $1 = 3 - 2$ sind I_1 und I_2 koprim. Also ist $Z[X] \oplus (I_1 \cap I_2) \cong I_1 \oplus I_2$. Andererseits ist weder I_1 noch I_2 als $\mathbb{Z}[X]$-Modul isomorph zu $\mathbb{Z}[X]$. Ansonsten wäre eines dieser Ideale ein Hauptideal. Wäre dies der Fall, so müsste der Erzeuger von I_1 ein Teiler von 2 und X und der Erzeuger von I_2 ein Teiler von 3 und X sein. Dann wäre aber $I_1 = R$ oder $I_2 = R$, was nicht der Fall ist.

Aufgabe 3.
Es ist schon bekannt, dass $\operatorname{End}(M)$ mit punktweiser Addition eine abelsche Gruppe bildet. Seien

$f,g,h \in \mathrm{End}(M)$ und $x,y \in M$ und $r \in R$. Es ist Es ist $(f \circ g)(x+y) = f(g(x+y)) = f(g(x)+g(y)) = f(g(x)) + f(g(y)) = (f \circ g)(x) + (f \circ g)(y)$, sowie $(f \circ g)(rx) = f(g(rx)) = f(r(g(x))) = rf(g(x)) = r(f \circ g)(x)$, was zeigt, dass $\mathrm{End}(M)$ abgeschlossen unter Verknüpfung ist. Weiter gilt offensichtlich $f \circ (g \circ h) = (f \circ g) \circ h$ sowie $(f+g) \circ h = (f \circ h) + (g \circ h)$. Es ist $f \circ \mathrm{id}_M = \mathrm{id}_M \circ f = f$, daher ist id_M das Einselement von $\mathrm{End}(M)$. Dies zeigt, dass $\mathrm{End}(M)$ mit $+$ und $\circ$ ein Ring ist.

Aufgabe 4.
Sei $t \in M$ ein Erzeuger von M. Dann ist die Abbildung

$$\begin{aligned} f\colon R &\longrightarrow M, \\ r &\longmapsto rt \end{aligned}$$

ein surjektiver R–Modulmorphismus. Sei $I = \ker(f)$. Dann ist $M \cong R/I$. Ist N ein Untermodul von M, so ist N isomorph zu einem Untermodul von R/I und somit isomorph zu einem Ideal $I \subseteq J \subseteq R$. Da R ein Hauptidealring ist, ist J und damit auch N zyklisch.

In beliebigen Ringen ist diese Aussage im Allgemeinen falsch. Man betrachte Beispielsweise $R = \mathbb{Z}[X]$ als Modul über sich selbst. Dieser ist sicherlich zyklisch erzeugt von 1. Allerdings ist das Ideal (bzw. der Untermodul) $(2,X) \subset \mathbb{Z}[X]$ kein Hauptideal und somit kein zyklischer $\mathbb{Z}[X]$–Modul.