Universität Konstanz
Fachbereich Mathematik und Statistik
Sommersemester 2011

Christoph Hanselka
Aaron Kunert
Markus Schweighofer

Lösungsblatt 6 zur Zahlentheorie

Aufgabe 1.
Wir zeigen zunächst, dass die Abbildungen in die richtigen Mengen gehen. In der Vorlesung wurde schon gezeigt, dass für fixiertes $f \in \mathrm{End}(M)$ die Multiplikation $p \cdot m := p(f)(m)$ für $p \in R[X]$ und $m \in M$, den Modul M zu einem $R[X]$–Modul macht. Weiter gilt für $r \in R$ auch $r \cdot m = r(f)(m) = r\,\mathrm{id}_M(m) = rm$, was zeigt, dass diese Modulstruktur eingeschränkt auf R, die ursprüngliche Modulstruktur ist. Sei nun M ein $R[X]$–Modul, so dass die $R[X]$–Operation die R–Operation erweitert. Zu zeigen ist, dass die Abbildung $\varphi\colon M \longrightarrow M$ mit $x \mapsto X \cdot x$ eine Endomorphismus von R–Moduln ist. Sei also $x,y \in M$ und $r \in R$. Dann ist $\varphi(x+y) = X \cdot (x+y) = X \cdot x + X \cdot y = \varphi(x) + \varphi(y)$. Weiter ist $\varphi(rx) = X \cdot (rx) = (rX) \cdot x = r(X \cdot x) = r\varphi(x)$. Man beachte, dass das zweite Gleichheitszeichen nur gilt, weil R als Teilmenge von $R[X]$ gerade die ursprüngliche Modulstruktur wiedergibt.

Nun ist noch zu zeigen, dass beide Zuordnungen hintereinanderausgeführt gerade die Identität auf den entsprechenden Mengen sind. Sei also $f \in \mathrm{End}(M)$. Die zugehörige Abbildung ist dann $\varphi\colon M \longrightarrow M$ mit $x \mapsto X \cdot x$. Dies ist jedoch $\varphi(x) = X \cdot x = f(x)$. Damit ist die eine Richtung gezeigt.

Sei nun $\odot$ eine $R[X]$–Modulmultiplikation, die die R–Modulstruktur fortsetzt. Sei $g \in \mathrm{End}(M)$ mit $g(x) = X \odot x$. Dann induziert g eine $R[X]$–Modulstruktur durch $p(x) \cdot m := p(g)(m)$ für $p \in R[X]$ und $m \in M$. Sei $p = \sum_{j=0}^{n} a_j X^j$. Dann ist

$$\begin{aligned} p \cdot m &= \sum_{i=0}^{n} a_j (g^j(m)) \\ &= \sum_{i=0}^{n} a_j (X^j \odot m) \\ &= \left(\sum_{i=0}^{n} a_j X^j \right) \odot m \\ &= p \odot m, \end{aligned}$$

was zeigt, dass wir die ursprüngliche $R[X]$–Modulstruktur zurückerhalten.

Aufgabe 2.
Nehmen wir zum Widerspruch an, dass $R := Z[\sqrt{5}]$ ein Hauptidealring ist. Dann ist R insbesondere faktoriell und damit ganz abgeschlossen. Auf der anderen Seite ist $\mathrm{qf}(R) = \mathbb{Q}(\sqrt{5}) =: K$. Wegen $5 \equiv_{(4)} 1$ ist $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ gerade der ganze Abschluss von $\mathbb{Z}$ in K. Damit ist $\frac{1+\sqrt{5}}{2}$ ganz über $\mathbb{Z}$ und somit insbesondere ganz über R. Wegen $\frac{1+\sqrt{5}}{2} \notin R$ ist dies ein Widerspruch zur ganzen Abgeschlossenheit von R. Somit kann R nicht faktoriell und damit kein Hauptidealring sein.

Aufgabe 3.
Sei M ein endlich erzeugter R–Modul und $f \in \mathrm{End}\, M$ surjektiv. Dann wird M ein (natürlich endlich erzeugter) $R[X]$–Modul durch $p \cdot m = p(f)(m)$ (für $p \in R[X]$ und $m \in M$). Sei $I = (X)$.

Da f surjektiv ist, ist $M = f(M) = IM$. Nun wenden wir den Satz von Cayley–Hamilton auf den Endomorphismus

$$\begin{aligned} \mathrm{id}\colon M &\longrightarrow M = IM, \\ x &\longmapsto x \end{aligned}$$

an. Es gibt daher also ein $n \in \mathbb{N}$ und $g_i \in I^i$ für $1 \leq i \leq n$ mit

$$m + g_1(m) + \ldots g_n(m) = 0 \quad \text{für alle } m \in M.$$

Man kann also annehmen, dass ein $g \in I$ existiert, mit $(m + g(m)) = 0$ für alle $m \in M$. Wegen $g \in I$ können wir $g = Xh$ für ein geeignetes $h \in R[X]$ schreiben. Ist nun $m \in \ker(f)$, so gilt $0 = (m + (hX)(m)) = (m + h(f(m))) = m$. Also ist $\ker(f) = 0$ und somit f injektiv.

Aufgabe 3.
Sei $A \subseteq B$ eine Erweiterung integrer Ringe. Nehmen wir zunächst an, dass A ein Körper ist. Dann ist zu zeigen, dass auch B ein Körper ist. Sei dazu $0 \neq x \in B$. Da x ganz über A ist, gibt es ein $n \in N$ und $a_1, \ldots, a_n \in A$ mit

$$x^n + a_1 x^{n-1} + \ldots a_n = 0.$$

Ist n mit dieser Eigenschaft minimal gewählt, so ist $a_n \neq 0$, denn sonst wäre

$$x(x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1}) = 0.$$

Da $x \neq 0$ und B ein Integritätsring ist, hätten wir somit eine Ganzheitsgleichung von x vom Grad $n-1$. Da also $a_n \neq 0$ und A ein Körper ist, folgt somit die Gleichung

$$\begin{aligned} \frac{x^n}{a_n} + \frac{a_1 x^{n-1}}{a_n} + \cdots + 1 &= 0 \\ 1 &= -\left(\frac{x^n}{a_n} + \frac{a_1 x^{n-1}}{a_n} + \cdots + x a_{n-1}\right) \\ 1 &= x\left(-\frac{x^{n-1}}{a_n} - \frac{a_1 x^{n-2}}{a_n} - \cdots - a_{n-1}\right). \end{aligned}$$

Dies zeigt, dass $x \in B$ invertierbar ist.

Sei nun B ein Körper, zu zeigen ist, dass auch A ein Körper ist. Sei $0 \neq x \in A$. Dann ist $\frac{1}{x} \in B$ ganz über A. Daher gibt es $a_1, \ldots, a_n \in A$ mit

$$\frac{1}{x^n} + \frac{a_1}{x^{n-1}} + \cdots + a_n = 0.$$

Multiplikation mit x^n liefert

$$1 = x\,(\underbrace{a_1 + \ldots a_n x^{n-1}}_{\in A}),$$

was zeigt, dass x schon in A invertierbar ist.