Fachbereich Mathematik
Prof. Dr. Nils Scheithauer
Walter Reußwig

TECHNISCHE UNIVERSITÄT DARMSTADT

WS 08/09 10. Februar 2009

Algebra

15. Übung mit Lösungshinweisen

Aufgabe 68 (Erzeugte Untermoduln) Sei R ein beliebiger Ring, M ein R-Modul und X eine beliebige Teilmenge von M. Zeige, daß der von X erzeugte Untermodul N vom M gleich der Menge

$$Y := \left\{ \sum_{i=1}^{s} r_i a_i + \sum_{j=1}^{t} n_j b_j \middle| s, t \in \mathbb{N}; a_i, b_j \in X, r_i \in R, n_j \in \mathbb{Z} \right\}$$

ist.
Zeige, daß, wenn R eine Eins besitzt und M unitär ist, der von X erzeugte Untermodul gleich der Menge

$$RX := \left\{ \sum_{k=1}^{s} r_i a_i \middle| s \in \mathbb{N}^+; a_i \in X; r_i \in R \right\}$$

ist.

LÖSUNG: Die Beweisstrategie: Wir zeigen zum einen, daß obige Menge ein Untermodul von M ist und zum anderen, daß jeder Untermodul, welcher X enthält, automatisch Y enthält.
Umsortieren der Summanden liefert sofort, daß aus $x, y \in Y$, auch $x - y \in Y$ folgt. Ebenso ist mit $r \in R$ und $x \in Y$ auch $rx \in Y$, da die Multiplikation von R und die Wirkung von $\mathbb{Z}$ auf M vertauschen: Es gilt immer

$$r \cdot n.x = r(x + x + ... + x) = rx + rx + ... + rx = (n.r)x.$$

Ist $\tilde{N}$ ein Untermodul von M mit $X \subseteq \tilde{N}$, so ist auch ra ein Element von $\tilde{N}$ mit $r \in R$ und $a \in X$. Weiter ist ebenfalls $n.a$ ein Element in $\tilde{N}$ mit $n \in \mathbb{Z}$. Somit liegen alle Elemente aus Y in $\tilde{N}$. Damit ist Y der kleinste Untermodul, welcher X enthält, also $Y = N$.
Im Falle eines unitären Moduls über einem Ring mit Eins setze $r_{s+j} := n_j$ und $a_{s+j} := b_j$ und laß die erste Summe von 1 bis $s + t$ laufen.

Aufgabe 69 (Isomorphiesätze) Sei R ein Ring, M ein R-Modul und N_1, N_2 Untermoduln von M. Zeige folgende Aussagen:

(a) Es gibt einen Isomorphismus $\alpha : N_1/(N_1 \cap N_2) \to (N_1 + N_2)/N_2$ mit

$$\alpha(x + N_1 \cap N_2) = x + N_2$$

für alle $x \in N_1$.

(b) Ist $N_2 \subseteq N_1$, so gibt es einen Isomorphismus $\beta : (M/N_2)/(N_1/N_2) \to M/N_1$ mit

$$\beta(x + N_2 + (N_1/N_2)) := x + N_1$$

für alle $x \in M$.

LÖSUNG: (a) Wir zeigen, daß α wohldefiniert ist. Ist $x = m + N_1 \cap N_2 = n + N_1 \cap N_2$ so folgt $m - n \in N_1 \cap N_2 \subseteq N_2$ und wir erhalten

$$\begin{aligned}
\alpha(x) &= \alpha(m + N_1 \cap N_2) \\
&= m + N_2 \\
&= m - n + n + N_2 \\
&= n + (m - n + N_2) \\
&= n + N_2 \\
&= \alpha(n + N_1 \cap N_2).
\end{aligned}$$

Somit ist die Definition unabhängig vom gewählten Repräsentanten. Die R-Linearität von α ist klar.

Weiter ist α injektiv: Sei $x = m + N_1 \cap N_2$ und $y = n + N_1 \cap N_2$. Aus der Gleichheit $\alpha(x) = \alpha(y)$ folgt, daß $m - n \in N_2$ gilt. Da m, n aus N_1 waren, erhalten wir somit $m - n \in N_1 \cap N_2$, also $x = y$.

Die Surjektivität von α erhalten wir wie folgt: Ist $m + N_2 \in (N_1 + N_2)/N_2$, so schreibe

$$m = a + b$$

mit $a \in N_1$ und $b \in N_2$. Dann folgt

$$m + N_2 = a + N_2.$$

Somit erhalten wir

$$\alpha(a + N_1 \cap N_2) = a + N_2 = m + N_2,$$

also ist α surjektiv. Damit ist α ein Isomorphismus.

(b) Auch β ist wohldefiniert. Ist $x = (a + N_2) + N_1/N_2 = (b + N_2) + N_1/N_2$, so folgt:

$$N_1/N_2 \ni a + N_2 - b - N_2 = (a - b) + N_2.$$

Somit gilt $a - b \in N_1$ und es folgt

$$\begin{aligned}
\beta((a + N_2) + N_1/N_2) &= a + N_1 \\
&= b + (a - b) + N_1 \\
&= b + N_1 \\
&= \beta((b + N_2) + N_1/N_2).
\end{aligned}$$

Somit ist β wohldefiniert. Die R-Linearität von β ist klar.

Wir rechnen Injektivität nach. Sei $\beta(x) = \beta(y)$ mit x, y bezeichnet wie oben. Dann sehen wir

$$\begin{aligned}
\beta(x) = \beta(y) &\Rightarrow a - b \in N_1 \\
&\Rightarrow a - b + N_2 \in N_1/N_2 \\
&\Rightarrow a - b + N_2 + N_1/N_2 = 0 + N_1/N_2 \\
&\Rightarrow a + N_2 + N_1/N_2 = b + N_2 + N_1/N_2 \\
&\Rightarrow x = y.
\end{aligned}$$

Wir rechnen Surjektivität nach. Sei $a + N_1 \in M/N_1$ beliebig. Dann erhalten wir

$$\beta(a + N_2) + N_1/N_2) = a + N_1,$$

also ist β surjektiv.

Aufgabe 70 (Nicht freie Moduln) Gib ein Beispiel eines nicht freien Moduls über einem Ring an.

LÖSUNG: Es ist $\mathbb{Z}_{42}$ ein nicht freier $\mathbb{Z}$-Modul, denn jedes Erzeugendensystem ist $\mathbb{Z}$-linear abhängig, denn für jede Menge $X \subseteq \mathbb{Z}_{42}$ und $x \in X$ gilt $42x = 0$, obwohl $42 \neq 0$ in $\mathbb{Z}$ gilt.

Aufgabe 71 (Endomorphismen) Zeige, daß es Isomorphismen $\mathrm{End}_{\mathbb{Z}}(\mathbb{Q}) \cong \mathbb{Q}$ und $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) \cong \{0\}$ gibt.

LÖSUNG: Sei $q \in \mathbb{Q}$ beliebig. Setze

$$\varphi_q(1) := q.$$

Diese Abbildung besitzt eine eindeutige Fortsetzung zu einem $\mathbb{Z}$-linearen Endomorphismus von $\mathbb{Q}$: Ist $n \in \mathbb{N}^{\times}$ beliebig, so muß gelten:

$$q = \varphi(1)_q = n \cdot \varphi_q\left(\frac{1}{n}\right).$$

Somit folgt

$$\varphi_q\left(\frac{1}{n}\right) = \frac{q}{n}.$$

Wir erhalten durch die Rechenregeln

$$\varphi_q(x+y) = (x+y)q = xq + yq = \varphi_q(x) + \varphi_q(y),$$

daß φ_q in der Tat ein Element aus $\mathrm{End}_{\mathbb{Z}}(\mathbb{Q})$ ist. Die Eindeutigkeit ist klar. Weiter gilt $\varphi_{q+r} = \varphi_q + \varphi_r$. Somit gibt es eine Injektion $\mathbb{Q} \to \mathrm{End}_{\mathbb{Z}}(\mathbb{Q})$. Umgekehrt ist ein beliebiger Endomorphismus ψ von der Form $\psi = \varphi_{\psi(1)}$, da $\psi(1) \in \mathbb{Q}$. Also folgt $\mathbb{Q} \cong \mathrm{End}_{\mathbb{Z}}(\mathbb{Q})$.
Ist $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z})$ ein nicht trivialer Homomorphismus, so gibt es ein $x \in \mathbb{Q}$ mit $\varphi(x) = n > 0$. Somit gilt

$$\varphi\left(\frac{x}{n}\right) = \frac{1}{n} \cdot \varphi(x) = 1.$$

Also gibt es ein Element $2y \in \mathbb{Q}$ mit $\varphi(2y) = 1$. Damit hätte die Gleichung

$$\varphi(y) + \varphi(y) = 1$$

in $\mathbb{Z}$ eine Lösung, ein Widerspruch. Also kann es diesen Homomorphismus nicht geben.

Aufgabe 72 (Kurzes Fünferlemma) Folgendes Diagramm habe exakte Zeilen und sei kommutativ

$$\begin{tikzcd}
0 \arrow[r] & M_1 \arrow[r, "\chi_1"] \arrow[d, "f"] & N_1 \arrow[r, "\sigma_1"] \arrow[d, "g"] & Q_1 \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & M_2 \arrow[r, "\chi_2"] & N_2 \arrow[r, "\sigma_2"] & Q_2 \arrow[r] & 0.
\end{tikzcd}$$

(a) Zeige folgende Aussagen:

 (1) Sind f und h surjektiv, so ist auch g surjektiv.

 (2) Sind f und h injektiv, so ist auch g injektiv.

 (3) Sind f und h Isomorphismen, so ist auch g ein Isomorphismus.

 Im Fall (3) heißen die beiden kurzen exakten Sequenzen *isomorph*.

(b) Zeige, daß für kurze exakte Sequenzen Isomorphie eine Äquivalenzrelation definiert.

LÖSUNG: (a) Wir zelebrieren die klassische Diagrammjagd.

(1) Seien f und h surjektiv. Wir wollen zeigen, ein beliebiges $n_2 \in N_2$ ist im Bild von f. Wir finden nun Elemente

$$q_2 := \sigma_2(n_2) \in Q_2, \quad q_1 \in Q_1 \text{ mit } h(q_1) = q_2 \text{ und } \quad n_1 \in N_1 \text{ mit } \sigma(n_1) = q_1.$$

Wir setzen $y := g(n_1) - n_2$. Nun jagen wir durchs andere Quadrat des Diagramms.
Aus $\sigma(y) = 0$ folgt $y = \chi_2(m_2)$ mit $m_2 \in M_2$. Da f surjektiv war, gibt es ein $m_1 \in M_1$ mit $f(m_1) = m_2$. Nun gilt

$$y = g(n_1) - n_2 = \chi_2(f(m_1)) = g(\chi_1(m_1)).$$

Somit erhalten wir

$$n_2 = g(n_1 - \chi_1(m_1)),$$

also ist g surjektiv.

(2) Seien f und h injektiv. Seien n_1 und n_1' Elemente aus N_1 mit $g(n_1) = g(n_1')$. Setze $y := n_1 - n_1'$. Wir zeigen, $y = 0$.
Aus $g(y) = 0$ folgt natürlich

$$h(\sigma_1(y)) = \sigma_2(g(y)) = 0.$$

Da h injektiv ist, ist $\sigma_1(y) = 0$, also existiert ein m_1 mit $\chi_1(m_1) = y$. Damit erhalten wir

$$\chi_2(f(m_1)) = g(\chi_1(m_1)) = g(y) = 0,$$

und da f und χ_2 injektiv waren, folgt $m_1 = 0$. Mit $0 = \chi_1(m_1) = y$, erhalten wir

$$n_1 = n_1',$$

also ist, wie behauptet, g injektiv.

(3) ist ein Korollar aus (1) und (2).

(b) Reflexivität und Transitivität sind klar: Im ersten Fall nehme jeweils die Identitäten, im letzteren Fall die Verknüpfung der Isomorphismen. Unklar ist die Symmetrie. Dazu zeigen wir, daß für ein gegebenes kommutatives Diagramm wie oben mit f, g, h Isomorphismen auch die inversen Isomorphismen das Diagramm kommutativ machen.
Sei m_2 aus M_2 beliebig, dann gilt

$$\chi_2(m_2) = \chi_2(f(f^{-1}(m_2))) = g(\chi_1(f^{-1}(m_2))).$$

Somit folgt

$$g^{-1}(\chi_2(m_2)) = \chi_1(f^{-1}(m_2)).$$

Es ist $h(\sigma_1(n_1)) = \sigma_2(g(n_1))$, also folgt

$$\sigma_1(n_1) = h^{-1}(\sigma_2(g(n_1))).$$

Mit $n_1 = g^{-1}(n_2)$ folgt

$$\sigma_1(g^{-1}(n_2)) = h^{-1}(\sigma_2(n_2)).$$

Somit ist das Diagramm mit den inversen Isomorphismen ebenfalls kommutativ, also ist Isomorphie kurzer exakter Sequenzen eine Äquivalenzrelation.

Aufgabe 73 (Elementarteilersatz) Sei $A = (a_{i,j})$ eine $n \times n$ - Matrix mit Einträgen in $\mathbb{Z}$. Setze für $1 \leq i \leq n$

$$w_i := (a_{i,1}, ..., a_{i,n})$$

und

$$N := \mathbb{Z}w_1 + ... + \mathbb{Z}w_n.$$

Zeige, daß $\mathbb{Z}^n/N$ genau dann endlich ist, wenn $\det(A) \neq 0$ gilt. In diesem Fall gilt weiter

$$|\mathbb{Z}^n/N| = |\det(A)|.$$

LÖSUNG: Sei $\mathbb{Z}^n/N$ endlich. Dann gibt es für jedes $\alpha \in \mathbb{Z}^n/N$ ein $m \in \mathbb{Z}$ mit $m\alpha = 0$, d.h. für jedes $\alpha \in \mathbb{Z}^n$ gibt es ein $m \in \mathbb{Z}$ mit $m\alpha \in N$. Jedes $\alpha \in \mathbb{Z}^n$ ist also im $\mathbb{Q}$-Spann der w_i, d. h. die w_i bilden eine $\mathbb{Q}$-Basis von $\mathbb{Q}^n \supseteq \mathbb{Z}^n$, also ist $\det(A) \neq 0$.
Sei $\det(A) \neq 0$. Dann sind die w_i linear unabhängig über $\mathbb{Q}$ und somit $\mathbb{Z}$-linear unabhängig. Somit folgt

$$N = \sum_{i=1}^{n} \mathbb{Z} w_i$$

hat Rang n. Nach dem Elementarteilersatz gibt es eine Basis $v_1, ..., v_n$ von $\mathbb{Z}^n$ und $a_1, ..., a_n \in \mathbb{Z}$ mit

$$N = \bigoplus_{i=1}^{n} \mathbb{Z} a_i v_i$$

und

$$\mathbb{Z}^n = \bigoplus_{i=1}^{n} \mathbb{Z} v_i.$$

Dann folgt

$$\mathbb{Z}^n/N = \bigoplus_{i=1}^{n} \mathbb{Z} vi/\mathbb{Z} a_i v_i = \bigoplus_{i=1}^{n} \mathbb{Z}/a_i\mathbb{Z},$$

d.h. $|\mathbb{Z}^n/N| = |a_1 \cdot ... \cdot a_n|$.
Wir beweisen nun den Zusatz: Definiere eine $n \times n$-Matrix über $\mathbb{Z}$ durch

$$w_i = \sum_{k=1}^{n} B_{i,k}(a_k v_k).$$

Da sich die $a_k v_k$ auch durch die w_j ausdrücken lassen, gibt es eine $n \times n$-Matrix C mit Einträgen in $\mathbb{Z}$ mit

$$a_k v_k = \sum_{j=1}^{n} C_{k,j} w_j.$$

Dann ist

$$\begin{aligned} w_i &= \sum_{j,k=1}^{n} B_{i,k} C_{k,j} w_j \\ &= \sum_{j=1}^{n} (BC)_{i,j} w_j, \end{aligned}$$

d. h.

$$BC = \mathbb{1}.$$

Somit folgt

$$\det(B) \in \pm 1.$$

Sei D die Matrix, deren Zeilen die v_j sind, also

$$D_{i,j} = (v_i)_j.$$

Sei M die Matrix

$$M = \operatorname{diag}(a_1, ..., a_n).$$

Dann ist

$$\begin{aligned} A_{i,j} &= (w_i)_j \\ &= (\sum_{k=1}^{n} B_{i,k}(a_k v_k))_j \\ &= \sum_{k=1}^{n} B_{i,k} a_k (v_k)_j \\ &= \sum_{k=1}^{n} B_{i,k} a_k D_{k,j} \\ &= \sum_{k=1}^{n} B_{i,k} (MD)_{k,j} \\ &= (BMD)_{i,j}. \end{aligned}$$

Somit erhalten wir

$$\begin{aligned} \det(A) &= \det(B)\det(M)\det(D) \\ &= \pm 1 \cdot (a_1 \cdot ... \cdot a_n) \cdot \pm 1, \end{aligned}$$

wobei $\det(D) \in \pm 1$ durch ein analoges Argument wie für B gewonnen werden kann. Somit folgt

$$|\det(A)| = |a_1 \cdot ... \cdot a_n| = |\mathbb{Z}^n / N|.$$