Lineare Algebra II – 11. Übungsblatt – Musterlösung

1. (a)⇒(b): Sei $I_1 \subset I_2 \subset \cdots$ eine aufsteigende Kette von Idealen. Setze

$$I := \bigcup \{I_j \mid j \in \mathbb{N}\}.$$

Wir wissen bereits, dass I ein Ideal von R ist. Seien $r_1, \dots, r_l \in \mathbb{R}$, sodass $I = r_1 R + \cdots + r_l R$. Für $1 \leq k \leq l$ gilt dann $r_k \in I$, also $r_k \in I_{j_k}$ für ein $j_k \in \mathbb{N}$. Sei $n := \max\{j_1, \dots, j_l\}$, dann gilt $r_k \in I_{j_k} \subset I_n$ für alle $1 \leq k \leq n$, also auch $I = r_1 R + \cdots + r_l R \subset I_n$. Für alle $k \geq n$ folgt dann

$$I_n \subset I_k \subset I \subset I_n,$$

also $I_n = I_k$.

(b)⇒(a): Sei $I \subset R$ nicht endlich erzeugt. Wir konstruieren eine unendliche aufsteigende Kette

$$r_1 R \subsetneq r_1 R + r_2 R \subsetneq r_1 R + r_2 R + r_3 R \subsetneq \cdots$$

von Idealen in R. Wähle $r_1 \in I$ beliebig. Dann gilt $r_1 R \subsetneq I$, da I nicht endlich erzeugt ist.

Seien $r_1, \dots, r_{n-1} \in I$ bereits gewählt. Dann gilt $r_1 R + \cdots + r_{n-1} R \subsetneq I$, da I nicht endlich erzeugt ist. Sei $r_n \in I \setminus (r_1 R + \cdots + r_{n-1} R)$. Dann folgt

$$r_1 R + \cdots + r_{n-1} R \subsetneq r_1 R + \cdots + r_n R.$$

2. (a) Seien $f, g, h \in \mathrm{End}(M)$ und $a, b \in M$. Da $(f+g)$ punktweise definiert ist, gilt

$$(f+g)(a+b) = f(a+b)+g(a+b) = f(a)+f(b)+g(a)+g(b) = (f+g)(a)+(f+g)(b).$$

Weiters gilt

$$(f\circ g)(a+b) = f(g(a+b)) = f(g(a)+g(b)) = f(g(a))+f(g(b)) = (f\circ g)(a)+(f\circ g)(b).$$

Daher sind $f+g$ und $f \circ g \in \mathrm{End}(M)$, und $+, \circ$ sind Verknüpfungen $\mathrm{End}(M) \times \mathrm{End}(M) \to \mathrm{End}(M)$.
Wir zeigen zunächst, dass $(\mathrm{End}(M), +)$ eine abelsche Gruppe ist. Assoziativität:

$$\begin{aligned}(f + (g+h))(a) &= f(a) + (g+h)(a) = f(a) + g(a) + h(a) = (f+g)(a) + h(a)\\ &= ((f+g)+h)(a).\end{aligned}$$

Kommutativität: $(f+g)(a) = f(a) + g(a) = g(a) + f(a) = (g+f)(a)$.
Weiters ist der Nullhomomorphismus $0 \in \mathrm{End}(M)$, der ganz M auf 0 abbildet, das neutrale Element: $(0+f)(a) = 0 + f(a) = f(a)$.

Sei $f \in \text{End}(M)$. Dann ist auch $-f : M \to M$, $(-f)(a) = -f(a)$ ein Endomorphismus von M, denn $(-f)(a+b) = -f(a+b) = -f(a) - f(b) = (-f)(a) + (-f)(b)$. Es gilt $(f + (-f))(a) = f(a) + (-f)(a) = f(a) - f(a) = 0 = 0(a)$, also ist $-f$ das inverse Element zu f.
Daher ist $(\text{End}(M), +)$ eine abelsche Gruppe. Weiters gilt

$$(f \circ (g \circ h))(a) = f((g \circ h)(a) = f(g(h(a))) = (f \circ g)(h(a)) = ((f \circ g) \circ h)(a),$$

also ist $\circ$ assoziativ. Distributivität:

$$\begin{aligned}(f \circ (g+h))(a) &= f((g+h)(a)) = f(g(a) + h(a)) = f(g(a)) + f(h(a)) \\ &= (f \circ g)(a) + (f \circ h)(a), \\ ((f+g) \circ h)(a) &= (f+g)(h(a)) = f(h(a)) + g(h(a)) = (f \circ h)(a) + (g \circ h)(a).\end{aligned}$$

Sei $\text{id}_M : M \to M$ die identische Abbildung. Dann gilt

$$(\text{id}_M \circ f)(a) = \text{id}_M(f(a)) = f(a) = f(\text{id}_M(a)) = (f \circ \text{id}_M)(a),$$

also ist $(\text{End}(M), +, \circ)$ ein Ring mit Einselement id_M.

(b) Wir definieren auf M die Skalarmultiplikation $\cdot : R \times M \to M$, $r \cdot m := \varphi(r)(m)$. Für $a, b \in R$, $m, n \in M$ gilt dann

$$\begin{aligned}a(bm) &= \varphi(a)(\varphi(b)(m)) = (\varphi(a) \circ \varphi(b))(m) = \varphi(ab)(m) = (ab)m, \\ (a+b)m &= \varphi(a+b)(m) = \varphi(a)(m) + \varphi(b)(m) = am + bm, \\ a(m+n) &= \varphi(a)(m+n) = \varphi(a)(m) + \varphi(a)(n) = am + an, \\ 1m &= \varphi(1)(m) = 1_{\text{End}_M}(m) = \text{id}_M(m) = m.\end{aligned}$$

Also ist M mit dieser Skalarmultiplikation ein R-Modul.

(c) Für $r \in R$ sei $\varphi(r) : M \to M$, $m \mapsto rm$. Dann gilt für $m, n \in M$:

$$\varphi(r)(m+n) = r(m+n) = rm + rn,$$

also ist $\varphi(r) \in \text{End}(M)$, und $\varphi : M \to \text{End}(M)$. Wir müssen noch zeigen, dass φ ein Ringhomomorphismus ist und $\varphi(1) = \text{id}_M$.
Für $a, b \in R$, $m \in M$ gilt

$$\begin{aligned}\varphi(a+b)(m) &= (a+b)m = am + bm = \varphi(a)(m) + \varphi(b)(m) = (\varphi(a) + \varphi(b))(m), \\ \varphi(ab)(m) &= abm = a(bm) = \varphi(a)(\varphi(b)(m)) = (\varphi(a) \circ \varphi(b))(m), \\ \varphi(1)(m) &= 1m = m = \text{id}_M(m),\end{aligned}$$

also $\varphi(a+b) = \varphi(a) + \varphi(b)$, $\varphi(ab) = \varphi(a) \circ \varphi(b)$, und $\varphi(1) = \text{id}_M$.

3. (a) Es gilt $0 = 0 + 0 \in N_1 + N_2$, für $n_1 + n_2 \in N_1 + N_2$ und $n_1' + n_2' \in N_1 + N_2$ ist auch $(n_1 + n_2) - (n_1' + n_2') = (n_1 - n_1') + (n_2 - n_2') \in N_1 + N_2$, also ist $N_1 + N_2$ eine Untergruppe von M. Für $r \in R$, $n_1 + n_2 \in N_1 + N_2$, ist auch $r(n_1 + n_2) = rn_1 + rn_2 \in N_1 + N_2$, also ist $N_1 + N_2$ ein Untermodul. Für $n_1 \in N_1$ folgt $n_1 = n_1 + 0 \in N_1 + N_2$, also $N_1 \subset N_1 + N_2$, und analog $N_2 \subset N_1 + N_2$.

   Wir haben gezeigt, dass $N_1 + N_2$ ein Untermodul von M ist, der $N_1 \cup N_2$ enthält. Da $\langle N_1 + N_2 \rangle$ der Durchschnitt aller solcher Untermoduln ist, folgt $\langle N_1 + N_2 \rangle \subset N_1 + N_2$.

   Sei umgekehrt $N \subset M$ ein beliebiger Untermodul, sodass $N_1 \cup N_2 \subset N$. Für $n_1 \in N_1$ und $n_2 \in N_1$ gilt dann $n_1, n_2 \in N$, also auch $n_1 + n_2 \in N$. Es folgt $N_1 + N_2 \subset M$. Daher ist $N_1 + N_2$ in jedem Untermodul enthalten, der $N_1 \cup N_2$ enthält, also auch im Durchschnitt all dieser Untermoduln. Es folgt $N_1 + N_2 \subset \langle N_1 \cup N_2 \rangle$.

   (b) Sei $L_1 : N_1 \to N_1 + N_2$ die Inklusion $n_1 \mapsto n_1$, und $L_2 : (N_1 + N_2) \to (N_1 + N_2)/N_2$ der natürliche Homomorphismus $m \mapsto m + N_2$. Beide dieser Abbildungen sind Homomorphismen, also auch

$$L = L_2 \circ L_1 : N_1 \to (N_1 + N_2)/N_2,\ n_1 \mapsto n_1 + N_2.$$

   L ist surjektiv: sei $m \in N_1 + N_2$, dann gibt es $n_1 \in N_1$, $n_2 \in N_2$, sodass $m = n_1 + n_2$, also $m + N_2 = n_1 + n_2 + N_2 = (n_1 + N_2) + (n_2 + N_2) = n_1 + N_2 = L(n_1)$. Sei $n \in N_1$. Dann gilt

$$L(n) = 0 \Leftrightarrow n + N_2 = 0 \Leftrightarrow n \in N_2 \Leftrightarrow n \in N_1 \cap N_2,$$

   also $\ker L = N_1 \cap N_2$.

   Nach dem Homomorphiesatz induziert L einen injektiven Homomorphismus

$$\tilde{L} : N_1/(N_1 \cap N_2) \to (N_1 + N_2)/N_2.$$

   Dieser ist surjektiv, da L surjektiv ist.

4. (a) $(\mathbb{Q}, +)$ ist nicht frei. Je zwei Elemente $a/b,\ c/d \in \mathbb{Q}$, mit $a, b, c, d \in \mathbb{Z}$, $b, d \neq 0$, sind linear abhängig: falls $a = 0$ oder $c = 0$, ist das klar. Ansonsten gilt

$$bc \cdot \frac{a}{b} - ad \cdot \frac{c}{d} = ca - ac = 0,$$

   und $bd, ad \neq 0$.

   Eine Basis B kann also nur ein Element haben. Für $a/b \in \mathbb{Q}$, $a, b \neq 0$ gilt aber $\langle a/b \rangle = \{na/b \mid n \in \mathbb{Z}\}$. Sei $p \in \mathbb{N}$, $p \nmid b$. Dann $1/p \in \mathbb{Q}$. Angenommen

$$\frac{1}{p} = n \cdot \frac{a}{b} = \frac{na}{b},$$

dann

$$0 = \frac{1}{p} - \frac{na}{b} = \frac{b - pna}{pb},$$

also $b = pna$, aber $p \nmid b$, ein Widerspruch. Daher folgt $\langle a/b \rangle \subsetneq \mathbb{Q}$, also kann es keine Basis mit nur einem Element geben.

(b) $(\mathbb{Q} \setminus \{0\}, \cdot)$ ist nicht frei. Sei $\odot : \mathbb{Z} \times \mathbb{Q} \to \mathbb{Q}$ die Skalarmultiplikation, d.h.

$$n \odot x = x^n, \qquad \text{für } n \in \mathbb{Z}, x \in \mathbb{Q}.$$

Für $2 \in \mathbb{Z}$ und $-1 \in \mathbb{Q}$ gilt dann

$$2 \odot -1 = (-1)^2 = 1,$$

und 1 ist das neutrale Element von $(\mathbb{Q} \setminus \{0\}, \cdot)$. Also ist $(\mathbb{Q} \setminus \{0\}, \cdot)$ als $\mathbb{Z}$-Modul nicht torsionsfrei, also nicht frei.

(c) $(\{x \in \mathbb{Q} \mid x > 0\}, \cdot)$ ist frei. Sei

$$B = \{p \mid p \text{ Primzahl}\}.$$

Dann ist B linear unabhängig: seien $p_1, \dots, p_k \in B$ paarweise verschieden und $n_1, \dots, n_k \in \mathbb{Z}$, mit

$$1 = (n_1 \odot p_1) \cdots (n_k \odot p_k) = p_1^{n_1} \cdots p_k^{n_k}.$$

Ohne Einschränkung der Allgemeinheit seien $n_1, \dots, n_l \geq 0$ und $n_{l+1}, \dots, n_k \leq 0$. Dann folgt

$$p_1^{n_1} \cdots p_l^{n_l} = p_{l+1}^{n_{l+1}} \cdots p_k^{n_k}.$$

Aufgrund der Eindeutigkeit der Primfaktorzerlegung in $\mathbb{N}$ kann das nur gelten, wenn $n_1 = \cdots = n_k = 0$.

B ist ein Erzeugendensystem: Sei $a/b \in \mathbb{Q}$, $a, b \in \mathbb{N}$, und seien $a = p_1^{n_1} \cdots p_k^{n_k}$, $b = q_1^{m_1} \cdots q_l^{m_l}$, mit Primzahlen $p_1, \dots, p_k, q_1, \dots, q_l$, und $n_1, \dots, n_k, m_1, \dots, m_l \in \mathbb{N}$. Dann folgt

$$\frac{a}{b} = \frac{p_1^{n_1} \cdots p_k^{n_k}}{q_1^{m_1} \cdots q_l^{m_l}} = (n_1 \odot p_1) \cdots (n_k \odot p_k) \cdot (-m_1 \odot q_1) \cdots (-m_l \odot q_l) \in \langle B \rangle.$$

Daher ist B eine Basis.