M. Künzer Abgabe im Ilias bis Do 18.04.2024 oder in der Übung

Homologische Algebra, SoSe 24

Blatt 1

Hausaufgabe 1 (cf. A3.(2), A8.(1))

Sei R ein Ring. Sei $I \subseteq R$ ein Ideal.

(1) Man zeige: Es wird $R/I := \{r + I \ : \ r \in R\}$ mittels $(r + I) + (r' + I) := (r + r') + I$ und $(r + I) \cdot (r' + I) := (r \cdot r') + I$ ein Ring.

(2) Man finde ein Ideal $I \subseteq \mathbb{Q}[X]$ und einen Ringisomorphismus $\mathbb{Q}[X]/I \xrightarrow{\sim} \mathbb{Q} \times \mathbb{Q}$.

(3) Sei $f : R \to S$ ein bijektiver Ringmorphismus.
Man zeige: Auch $f^{-1} : S \to R$ ist ein Ringmorphismus.

Lösung.
Zu (1).
Wohldefiniertheit von $(+)$:
Seien r, $\tilde{r}$, r', $\tilde{r}' \in R$ gegeben mit $r + I = \tilde{r} + I$ und $r' + I = \tilde{r}' + I$. Zu zeigen ist: $(r + r') + I \overset{!}{=} (\tilde{r} + \tilde{r}') + I$.
Es ist $r - \tilde{r} \in I$ und $r' - \tilde{r}' \in I$. Also ist $(r + r') - (\tilde{r} + \tilde{r}') = (r - \tilde{r}) + (r' - \tilde{r}') \in I$, d.h. $(r + r') + I = (\tilde{r} + \tilde{r}') + I$.
Wohldefiniertheit von $(\cdot)$: Seien r, $\tilde{r}$, r', $\tilde{r}' \in R$ gegeben mit $r + I = \tilde{r} + I$ und $r' + I = \tilde{r}' + I$. Zu zeigen ist: $(r \cdot r') + I \overset{!}{=} (\tilde{r} \cdot \tilde{r}') + I$.
Es ist $r - \tilde{r} \in I$ und $r' - \tilde{r}' \in I$. Also ist $rr' - \tilde{r}\tilde{r}' = rr' - r\tilde{r}' + r\tilde{r}' - \tilde{r}\tilde{r}' = r(r' - \tilde{r}') + (r - \tilde{r})\tilde{r}' \in I$, d.h. $(r \cdot r') + I = (\tilde{r} \cdot \tilde{r}') + I$.
Im folgenden schreiben wir kurz $[r] := r + I$ für $r \in R$.
(Ring 1): Es ist $(R/I, +)$ die bekannte additive Faktorgruppe.
(Ring 2): Für r, s, $t \in R$ ist

$$[r] \cdot ([s] \cdot [t]) \ = \ [r] \cdot [s \cdot t] \ = \ [r \cdot (s \cdot t)] \ = \ [(r \cdot s) \cdot t] \ = \ [r \cdot s] \cdot [t] \ = \ ([r] \cdot [s]) \cdot [t] \, .$$

(Ring 3): Für $r \in R$ ist

$$[r] \cdot [1_R] \ = \ [r \cdot 1_R] \ = \ [r] \ = \ [1_R \cdot r] \ = \ [1_R] \cdot [r] \, .$$

Insbesondere ist $1_{R/I} = [1_R] = 1_R + I$.
(Ring 4): Seien r, r', s, $s' \in R$. Zum einen wird

$$[r] \cdot ([s] + [s']) \ = \ [r] \cdot [s + s'] \ = \ [r \cdot (s + s')] \ = \ [r \cdot s + r \cdot s'] \ = \ [r \cdot s] + [r \cdot s'] \ = \ [r] \cdot [s] + [r] \cdot [s'] \, .$$

Zum anderen wird

$$([r] + [r']) \cdot [s] \ = \ [r + r'] \cdot [s] \ = \ [(r + r') \cdot s] \ = \ [r \cdot s + r' \cdot s] \ = \ [r \cdot s] + [r' \cdot s] \ = \ [r] \cdot [s] + [r'] \cdot [s] \, .$$

Zu (2). Sei $\varphi : \mathbb{Q}[X] \to \mathbb{Q} \times \mathbb{Q} : X \mapsto (1, 0)$. Dann bildet φ das Element $f(X) \in \mathbb{Q}[X]$ auf $(f(1), f(0))$ ab. Es ist also $\mathrm{Kern}(\varphi) = \mathbb{Q}[X](X - 1) \cap \mathbb{Q}[X]X = \mathbb{Q}[X](X - 1)X =: I$.
Es ist φ surjektiv, da für a, $b \in \mathbb{Q}$ das Element $aX + b(1 - X)$ auf (a, b) abgebildet wird.
Dank Homomorphiesatz ist also $\bar{\varphi} : \mathbb{Q}[X]/I \to \mathbb{Q} \times \mathbb{Q} : f(X) + I \mapsto (f(1), f(0))$ ein Isomorphismus.

Zu (3). Es ist

$$(r + s)f^{-1} \ = \ (rf^{-1}f + sf^{-1}f)f^{-1} \ = \ (rf^{-1} + sf^{-1})ff^{-1} \ = \ rf^{-1} + sf^{-1}$$

und

$$(r \cdot s)f^{-1} \ = \ (rf^{-1}f \cdot sf^{-1}f)f^{-1} \ = \ (rf^{-1} \cdot sf^{-1})ff^{-1} \ = \ rf^{-1} \cdot sf^{-1}$$

für r, $s \in R$. Ferner ist

$$1_S f^{-1} \ = \ 1_R ff^{-1} \ = \ 1_R \, .$$

Hausaufgabe 2 (cf. A7)

Sei R ein Ring. Sei M ein R-Linksmodul. Sei $N \subseteq M$ ein Teilmodul.

(1) Man zeige: Es ist M/N via $(m+N)+(m'+N) := (m+m')+N$ für $m,\, m' \in M$ und via $r \cdot (m+N) := (r \cdot m)+N$ für $r \in R$ und $m \in M$ ein R-Linksmodul.

(2) Man zeige: Ist M als Menge endlich, dann ist $|N| \cdot |M/N| = |M|$.

Lösung.
Zu (1).
Wohldefiniertheit von $(+)$: Seien $m,\, \tilde{m},\, m',\, \tilde{m}' \in M$ gegeben mit $m+N = \tilde{m}+N$ und mit $m'+N = \tilde{m}'+N$. Zu zeigen ist: $m+m'+N \overset{!}{=} \tilde{m}+\tilde{m}'+N$.
Aus $m-\tilde{m} \in N$ und $m'-\tilde{m}' \in N$ folgt $(m+m')-(\tilde{m}+\tilde{m}') = (m-\tilde{m})+(m'-\tilde{m}') \in N$, i.e. $m+m'+N = \tilde{m}+\tilde{m}'+N$.
Wohldefiniertheit von $(\cdot)$: Seien $m,\, \tilde{m} \in M$ gegeben mit $m+N = \tilde{m}+N$. Sei $r \in R$. Zu zeigen ist: $rm+N \overset{!}{=} r\tilde{m}+N$.
Aus $m-\tilde{m} \in N$ folgt $rm - r\tilde{m} = r(m-\tilde{m}) \in N$, i.e. $rm+N = r\tilde{m}+N$.
Im folgenden schreiben wir kurz $[m] := m+N$ für $m \in M$.
(LMod 1): Es ist $(M/N, +)$ die bekannte additive Faktorgruppe.
(LMod 2): Seien $r,\, s \in R$ und $m \in M$. Es wird

$$(r \cdot s)\cdot[m] \;=\; [(r\cdot s)\cdot m] \;=\; [r\cdot(s\cdot m)] \;=\; r\cdot[s\cdot m] = r\cdot(s\cdot[m])\,.$$

(LMod 3): Sei $m \in M$. Es wird

$$1\cdot[m] \;=\; [1\cdot m] \;=\; [m]\,.$$

(LMod 4): Seien $r,\, r' \in R$ und $m,\, m' \in M$. Es wird

$$(r+r')\cdot[m] \;=\; [(r+r')\cdot m] \;=\; [r\cdot m + r'\cdot m] \;=\; [r\cdot m]+[r'\cdot m] \;=\; r\cdot[m]+r'\cdot[m]$$

und

$$r\cdot([m]+[m']) \;=\; r\cdot[m+m'] \;=\; [r\cdot(m+m')] \;=\; [r\cdot m + r\cdot m'] \;=\; [r\cdot m]+[r\cdot m'] \;=\; r\cdot[m]+r\cdot[m']\,.$$

Zu (2). Sei $k := |M/N|$. Wir wählen Repräsentanten $m_1,\ldots,m_k \in M$ der Restklassen modulo N. Es ist also $M = \bigsqcup_{i\in[1,k]}(m_i+N)$.
Für $i \in [1,k]$ ist $|m_i+N| = |N|$, da die Abbildung $N \to m_i+N : n \mapsto m_i+n$ bijektiv ist.
Folglich ist

$$|M| \;=\; \sum_{i\in[1,k]} |m_i+N| \;=\; \sum_{i\in[1,k]} |N| \;=\; |N|\cdot k \;=\; |N|\cdot|M/N|\,.$$

Hausaufgabe 3

(1) Sei $R = (R, +_R, \cdot_R)$ ein Ring. Sei $R^\circ = (R^\circ, +_{R^\circ}, \cdot_{R^\circ})$ der Ring, für welchen $(R^\circ, +_{R^\circ}) = (R, +_R) =: (R,+)$ ist und für welchen $r \cdot_{R^\circ} s = s \cdot_R r$ gilt für $r,\, s \in R$.

Sei nun $R = \mathbb{Q}^{2\times 2}$. Man finde einen Ringisomorphismus $f : R \to R^\circ$.

(2) Sei R ein Ring. Sei $M = (M,+)$ eine abelsche Gruppe.

Sei $\mathrm{End}_{\mathbb{Z}}(M) = \{\, M \xrightarrow{f} M \;:\; f \text{ ist Gruppenmorphismus} \,\}$ der Endomorphismenring von M. Darin werde $f+g$ durch $m(f+g) := mf + mg$ definiert für $f,\, g \in \mathrm{End}_{\mathbb{Z}}(M)$. Die Multiplikation ist gegeben durch die Komposition.

Sei $\varphi : R^\circ \to \mathrm{End}_{\mathbb{Z}}(M)$ ein Ringmorphismus. Man zeige: Vermittels $r\cdot m := m(r\varphi)$ wird M zu einem R-Linksmodul.

Lösung.
Zu (1). Es ist die Transpositionsabbildung

$$f : R \to R^\circ : A \mapsto A^{\mathrm{t}}$$

ein Ringisomorphismus. Denn zum einen ist

$$1_R f \;=\; \mathrm{E}_2^{\mathrm{t}} \;=\; \mathrm{E}_2 \;=\; 1_{R^\circ}\ .$$

Zum anderen ist für $A, B \in R$

$$(A +_R B)f \;=\; (A+B)^{\mathrm{t}} \;=\; A^{\mathrm{t}} + B^{\mathrm{t}} \;=\; Af +_{R^\circ} Bf$$

und

$$(A \cdot_R B)f \;=\; (AB)^{\mathrm{t}} \;=\; B^{\mathrm{t}} A^{\mathrm{t}} \;=\; A^{\mathrm{t}} \cdot_{R^\circ} B^{\mathrm{t}} \;=\; Af \cdot_{R^\circ} Bf\ .$$

Da $(A^{\mathrm{t}})^{\mathrm{t}} = A$ für $A \in R$, ist f bijektiv.
Insgesamt ist f also ein Ringisomorphismus.

Zu (2).
(LMod 1): Es ist $(M, +)$ eine abelsche Gruppe.
(LMod 2): Seien $r, s \in R$. Sei $m \in M$. Es wird

$$(r \cdot_R s) \cdot m \;=\; m((r \cdot_R s)\varphi) \;=\; m((s \cdot_{R^\circ} r)\varphi) \;=\; m(s\varphi \cdot r\varphi) \;=\; (m(s\varphi))(r\varphi) \;=\; (s \cdot m)(r\varphi) \;=\; r \cdot (s \cdot m)\ .$$

(LMod 3): Sei $m \in M$. Es wird

$$1 \cdot m \;=\; m(1_R\varphi) \;=\; m(1_{R^\circ}\varphi) \;=\; m1_{\mathrm{End}_{\mathbb{Z}}(M)} \;=\; m\,\mathrm{id}_M \;=\; m\ .$$

(LMod 4): Seien $r, r' \in R$ und $m, m' \in M$. Es wird

$$(r + r') \cdot m \;=\; m((r + r')\varphi) \;=\; m(r\varphi + r'\varphi) \;=\; m(r\varphi) + m(r'\varphi) \;=\; r \cdot m + r' \cdot m$$

und

$$r \cdot (m + m') \;=\; (m + m')(r\varphi) \;=\; m(r\varphi) + m'(r\varphi) \;=\; r \cdot m + r \cdot m'\ .$$

Hausaufgabe 4 (cf. A10)

Seien $m,\, n \geqslant 0$. Sei $A \in \mathbb{Z}^{m\times n}$.

(1) Man zeige: Falls $m,\, n \geqslant 1$, dann gibt es ganzzahlig invertierbare Matrizen $S \in \mathbb{Z}^{m\times m}$ und $T \in \mathbb{Z}^{n\times n}$, für welche SAT von der Blockmatrixform $\left(\begin{smallmatrix} a & 0 \\ 0 & A' \end{smallmatrix}\right)$ ist, wobei $a \in \mathbb{Z}$ ein Teiler jedes Eintrags von $A' \in \mathbb{Z}^{(m-1)\times(n-1)}$ ist.

(2) Man zeige: Es gibt ganzzahlig invertierbare Matrizen $S \in \mathbb{Z}^{m\times m}$ und $T \in \mathbb{Z}^{n\times n}$, für welche SAT eine Matrix ist, deren Einträge an jeder Position $(i, j) \in [1, m] \times [1, n]$ mit $i \neq j$ gleich 0 sind (rechteckige Diagonalmatrix) und deren Eintrag an Position (i, i) den Eintrag an Position $(i + 1, i + 1)$ teilt für $i \in [1, \min\{m, n\} - 1]$.

Zu (1).
Eine Matrix in $\mathbb{Z}^{m\times m}$ oder $\mathbb{Z}^{n\times n}$ heißt hier ganzzahlig invertierbar oder kurz invertierbar, falls sie ein Inverses mit Einträgen aus $\mathbb{Z}$ besitzt.
Eine Zeilenvertauschung in einer Matrix in $\mathbb{Z}^{m\times n}$ entspricht einer Multiplikation mit einer invertierbaren Matrix von links.
Die Addition eines ganzzahligen Vielfachen einer Zeile zu einer anderen in einer Matrix in $\mathbb{Z}^{m\times n}$ entspricht einer Multiplikation mit einer invertierbaren Matrix von links.
Analog für Spaltenoperationen.
Wir wollen zeigen, daß es $S \in \mathbb{Z}^{m\times m}$ invertierbar und $T \in \mathbb{Z}^{n\times n}$ invertierbar so gibt, daß $SAT = \left(\begin{smallmatrix} a & 0 \\ 0 & A' \end{smallmatrix}\right)$ für ein $a \in \mathbb{Z}$ und ein $A' \in \mathbb{Z}^{(m-1)\times(n-1)}$, wobei a' jeden Eintrag von A' teilt.

Wir zeichnen folgende Teilmenge und folgendes Element der Menge $[1,m] \times [1,n]$ aller Eintragspositionen der Matrizen in $\mathbb{Z}^{m\times n}$ aus.

Sei $\{(i,1) \;:\; i \in [2,m]\} \cup \{(1,j) \;:\; j \in [2,n]\} \subseteq [1,m] \times [1,n]$ der *Rand.*

Sei $(1,1) \in [1,m] \times [1,n]$ das *Eck.*

Wir verfahren wie folgt.

1. Falls $A = 0$ ist, so sind wir fertig.

Falls $A \neq 0$ ist, so tauschen wir den betragskleinsten Eintrag ungleich 0 von A ins Eck.

2. Für alle Einträge im Rand, die ungleich 0 sind, erreichen wir unter Verwendung einer Addition eines Vielfachen der ersten Zeile zur betreffenden Zeile oder unter Verwendung einer Addition eines Vielfachen der ersten Spalte zur betreffenden Spalte, daß alle Einträge im Rand betragskleiner sind als der Eintrag im Eck.

3. Falls nun alle Einträge im Rand gleich 0 sind, so springen wir zu 4.

Falls es einen Eintrag im Rand gibt, der ungleich 0 ist, so tauschen wir diesen ins Eck und springen zu 2.

4. Nun sind alle Einträge im Rand gleich 0.

Falls der Eintrag im Eck nicht alle Einträge von A teilt, so tauschen wir einen Eintrag von A, der nicht geteilt wird, in die erste Spalte und springen nach 2.

Falls der Eintrag im Eck alle Einträge von A teilt, so sind wir fertig.

Falls von 3. nach 2. gesprungen wird, wird das Eck echt betragskleiner.

Falls von 4. nach 2. gesprungen wird, wird dann in 3. das Eck echt betragskleiner.

Daher terminiert dieses Vorgehen.

Zu (2). Wir verfahren per Induktion über $\min\{n,m\}$.

Ist $\min\{n,m\} = 0$, so ist nichts zu zeigen.

Sei $\min\{n,m\} \geqslant 1$. Dank (1) finden wir invertierbare Matrizen $S' \in \mathbb{Z}^{m\times m}$ und $T' \in \mathbb{Z}^{n\times n}$, für welche $S'AT'$ von der Blockmatrixform $\left(\begin{smallmatrix} a & 0 \\ 0 & A' \end{smallmatrix}\right)$ ist, wobei $a \in \mathbb{Z}$ ein Teiler jedes Eintrags von $A' \in \mathbb{Z}^{(m-1)\times(n-1)}$ ist.

Also: $S'AT' = \left(\begin{smallmatrix} a & 0 \\ 0 & A' \end{smallmatrix}\right)$.

Dank Induktionsvoraussetzung finden wir invertierbare Matrizen $S'' \in \mathbb{Z}^{(m-1)\times(m-1)}$ und $T'' \in \mathbb{Z}^{(n-1)\times(n-1)}$, für welche $S''A'T'' = D$ ist, wobei in D die Einträge an jeder Position $(i,j) \in [1,m-1]\times[1,n-1]$ mit $i \neq j$ gleich 0 sind (rechteckige Diagonalmatrix) und deren Eintrag an Position (i,i) den Eintrag an Position $(i+1,i+1)$ teilt für $i \in [1, \min\{m-1, n-1\} - 1]$.

Also: $S''A'T'' = D$.

Da a jeden Eintrag von A' teilt, teilt a auch jeden Eintrag von $S''A'T'' = D$.

Sei $S := \left(\begin{smallmatrix} 1 & 0 \\ 0 & S'' \end{smallmatrix}\right) \cdot S'$. Sei $T := T' \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & T'' \end{smallmatrix}\right)$. Es wird

$$SAT \;=\; \left(\begin{smallmatrix} 1 & 0 \\ 0 & S'' \end{smallmatrix}\right) \cdot S'AT' \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & T'' \end{smallmatrix}\right) \;=\; \left(\begin{smallmatrix} 1 & 0 \\ 0 & S'' \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} a & 0 \\ 0 & A' \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & T'' \end{smallmatrix}\right) \;=\; \left(\begin{smallmatrix} a & 0 \\ 0 & S''A'T'' \end{smallmatrix}\right) \;=\; \left(\begin{smallmatrix} a & 0 \\ 0 & D \end{smallmatrix}\right) \;,$$

und dies ist eine Matrix wie in (2) gewünscht.