Lösung 12

Freie Moduln, Klassifikation endlich erzeugter Moduln über Hauptidealringen, Elementarteiler

1. (a) Zeigen Sie, dass $\mathbb{Q}$ ein torsionsfreier $\mathbb{Z}$-Modul ist, der nicht endlich erzeugt und nicht frei ist.

   (b) Sei M ein freier Modul von endlichem Rang über einem beliebigen Hauptidealring. Beweisen oder widerlegen Sie (anhand eines konkreten Beispiels):

      i. Jede linear unabhängige Teilmenge von M lässt sich zu einer Basis von M ergänzen.

      ii. Aus jedem Erzeugendensystem von M lässt sich eine Basis von M auswählen.

2. Finden Sie die Smith Normalform und die zugehörigen Matrizen g, h für die Matrix

$$A := \begin{pmatrix} 4 & 7 \\ 5 & 8 \\ 6 & 9 \end{pmatrix} \in \mathbb{Z}^{3\times 2}.$$

   Geben Sie einen expliziten Isomorphismus von $\mathbb{Z}^3/A\mathbb{Z}^2$ auf ein direktes Produkt von zyklischen Gruppen an.

3. (a) Bestimmen Sie alle Isomorphieklassen von abelschen Gruppen der Ordnung 600.

   (b) Bestimmen Sie alle Isomorphieklassen von $\mathbb{F}_2[X]$-Moduln der Ordnung, d.h. der Kardinalität 16.

   Hinweis: Verwenden Sie Aufgabe 3 der Serie 6.

Sei M ein endlich erzeugter Torsionsmodul über einem Hauptidealring. Nach dem zweiten Teil des Klassifikationssatzes wissen wir, dass $d_1 \mid \ldots \mid d_n \in R \smallsetminus \{0\}$ existieren, so dass

$$M \cong R/(d_1) \times \cdots \times R/(d_n).$$

Die Elemente $d_1, \ldots, d_n$ werden *Elementarteiler von M* genannt. In den folgenden zwei Aufgaben werden wir den Beweis des zweiten Teils des Klassifikationssatzes vervollständigen und zeigen, dass die Elementarteiler bis auf Assoziertheit eindeutig durch M bestimmt sind.

4. Sei M ein Torsionsmodul über einem Hauptidealring R. Wir nehmen an, es existiert $d \in R$ mit $dm = 0$ für alle $m \in M$, d.h. M wird von d *annihiliert*. Sei $d =$

$p_1^{n_1} \cdot \ldots \cdot p_m^{n_m}$ für inäquivalente Primelemente $p_1, \ldots, p_m \in R$ und $n_1, \ldots, n_m \in \mathbb{N}$. Zeigen Sie, dass

$$M = \bigoplus_{i=1}^{m} M_{p_i},$$

wobei $M_{p_i} = \{m \in M \mid (p_i)^{n_i} m = 0\}$.

Hinweis: Betrachten Sie zuerst den Fall $d = a_1 a_2$ mit a_1, a_2 koprim. Dann existieren b_1, b_2 mit $1 = a_1 b_1 + a_2 b_2$. Betrachten Sie $M_i = \ker(M \to M, m \mapsto a_i m)$ und zeigen Sie, dass $M = M_1 \oplus M_2$.

5. Sei M ein endlich erzeugter Torsionsmodul über einem Hauptidealring R der von p^n annihiliert wird, wobei $p \in R$ prim und $n \in \mathbb{N}$. Zeigen Sie, dass die Elementarteiler wie sie im zweiten Teil des Klassifikationssatzes auftreten p-Potenzen sind und bis auf Assoziertheit eindeutig durch M bestimmt sind.

   Hinweis: Betrachten Sie $p^j M / p^{j+1} M$, $j = 0, \ldots, n-1$.

   Lösung: Sei M ein endlich erzeugter R-Torsionsmodul und seien $e_1 | e_2 | \ldots | e_n \in R$ Elementarteiler von M, also

$$M \cong \bigoplus_{i=1}^{n} R/e_i R.$$

   Da p^n den Modul M annihiliert, annihiliert p^n auch $R/e_i R$ für alle $i = 1, \ldots, n$. Das heisst aber nichts anderes, als, dass $p^n R \subseteq e_i R$ und daraus folgt $e_i \mid p^n$ für alle $i = 1, \ldots, n$. Wir wissen nun, dass bis auf Assoziiertheit $e_i = p^{k_i}$ mit $k_1 \leqslant k_2 \leqslant \ldots \leqslant n$ (nach der eindeutigen Zerlegung in Primelemente bis auf Assoziiertheit). Das heisst jedes der e_i ist bis auf Assoziiertheit durch j_i eindeutig bestimmt, und damit sind die Elementarteiler durch die Zahlen

$$\#\{1 \leqslant i \leqslant n : p^j | p^{k_i}\}$$

   für $j = 1, \ldots, n$ bestimmt.

   Wir wollen nun den Hinweis betrachten.

   Bemerkung: Für jedes $p \in R$ prim und $j \geqslant 0$ ist $p^j M / p^{j+1} M$ ein R/pR-Vektorraum.

   Beweis: Als Faktormodul eines Untermoduls von M ist $p^j M / p^{j+1} M$ ein R-Modul. Für jedes $x \in pR$ und $m \in p^j M$ gilt $xm \in p^{j+1} M$, also $x[m] = 0_{p^j M / p^{j+1} M}$. Also induziert die Operation von R auf $p^j M / p^{j+1} M$ eine wohl-definierte Operation von R/pR auf $p^j M / p^{j+1} M$, bezüglich der $p^j M / p^{j+1} M$ ein R/pR-Modul ist (und somit ein R/pR-Vektorraum, da R/pR ein Körper ist). □

   Lemma: Seien $e \in R$ und $N := R/eR$. Dann ist

$$\dim_{R/pR}(p^j N / p^{j+1} N) = \begin{cases} 1, & p^{j+1} | e \\ 0, & \text{sonst.} \end{cases}$$

Beweis: Es gilt

$$\begin{aligned} p^jN/p^{j+1}N &= \big(p^j(R/eR)\big)\big/\big(p^{j+1}(R/eR)\big) \\ &\cong \big(p^jR/(p^jR\cap eR)\big)\big/\big(p^{j+1}R/(p^{j+1}R\cap eR)\big) \\ &= (p^jR/\mathrm{kgV}(p^j,e)R)/(p^{j+1}R/\mathrm{kgV}(p^{j+1},e)R). \end{aligned}$$

Falls $p^{j+1}|e$ gilt, so ist $\mathrm{kgV}(p^j,e)=\mathrm{kgV}(p^{j+1},e)=e$, und somit

$$p^jN/p^{j+1}N \cong (p^jR/eR)/(p^{j+1}R/eR) \cong p^jR/p^{j+1}R \cong R/pR,$$

also ist in diesem Fall $\dim_{R/pR}(p^jN/p^{j+1}N)=\dim_{R/pR}(R/pR)=1$.

Falls $p^{j+1}\nmid e$ gilt, so ist $\mathrm{kgV}(p^{j+1},e)=p\cdot\mathrm{kgV}(p^j,e)$, und mit $a:=\mathrm{kgV}(p^j,e)$ gilt somit

$$p^jN/p^{j+1}N \cong (p^jR/aR)/(p^{j+1}R/paR) \cong R/R \cong \{0\},$$

also ist in diesem Fall $\dim_{R/pR}(p^jN/p^{j+1}N)=0$. □

Wir schliessen mit dem folgenden Korollar.

Korollar:

$$\dim_{R/pR}(p^jM/p^{j+1}M) = \#\{1\leqslant k\leqslant n : p^{j+1}|p^{k_i}\}.$$

Beweis: Für $1\leqslant i\leqslant n$ sei $N_i := R/p^{k_i}R$. Es gilt

$$p^jM/p^{j+1}M \cong p^j\Big(\bigoplus_{i=1}^n N_i\Big)\Big/p^{j+1}\Big(\bigoplus_{i=1}^n N_i\Big) \cong \bigoplus_{i=1}^n p^jN_i/p^{j+1}N_i,$$

also

$$\dim_{R/pR}(p^jM/p^{j+1}M) = \sum_{i=1}^n \dim_{R/pR}(p^jN_i/p^{j+1}N_i),$$

und die Behauptung folgt aus dem Lemma. □

Die Dimension $\dim_{R/pR}(p^jM/p^{j+1}M)$ hängt aber nur von M ab und nicht von der Wahl der Elementarteiler $e_1,\ldots,e_n$; nach der obigen Feststellung sind die Elementarteiler von M also bis auf Einheiten eindeutig.

6. Sei R ein vom Nullring verschiedener Ring und sei G eine Gruppe. Wir definieren den *Gruppenring* $R[G]$ als Menge der endlichen formalen R-Linearkombinationen von Elementen aus G

$$R[G] := \Big\{\sum_{g\in G} r_g g \;\Big|\; r_g\in R \text{ und } r_g=0 \text{ für fast alle } g\in G\Big\}$$

mit Addition

$$\Big(\sum_{g\in G} r_g g\Big)+\Big(\sum_{g\in G} s_g g\Big) := \sum_{g\in G}(r_g+s_g)g$$

und dem "Faltungsprodukt"

$$\Big(\sum_{g\in G} r_g g\Big)\cdot\Big(\sum_{g\in G} s_g g\Big) := \sum_{g\in G}\Big(\sum_{hk=g} r_h s_k\Big)g.$$

(a) Zeigen Sie, dass $(R[G], +, \cdot)$ ein (nicht notwendigerweise kommutativer) Ring ist.

(b) Wann ist $R[G]$ kommutativ?

(c) Zeigen Sie, dass $R[G]$ nicht nullteilerfrei ist, falls G ein nicht-triviales Element von endlicher Ordnung enthält.

(d) Zeigen Sie, dass $R[\mathbb{Z}/2\mathbb{Z}] \cong R \times R$ ist, falls 2 in R invertierbar ist.

(e) Konstruieren Sie eine natürliche Bijektion zwischen der Menge der Gruppenhomomorphismen $G \to R^\times$ und der Menge der Ringhomomorphismen $\mathbb{Z}[G] \to R$.

(f) Zeigen Sie, dass $R[\mathbb{Z}] \cong R[X,Y]/(1-XY)$ und $R[\mathbb{Z}/n\mathbb{Z}] \cong R[X]/(X^n-1)$ sind.

Lösung:

(a) Das Elemente $\sum_{g\in G} 0\, g$ ist das neutrale Element bezüglich Addition und $1_R\, e_G + \sum_{g\in G, g\neq e_G} 0\, g$ ist das neutrale Element bezüglich Multiplikation in $R[G]$. Das additive Inverse eines Elements $\sum_{g\in G} r_g\, g$ ist das Element $\sum_{g\in G}(-r_g)\, g$, wobei $-r_g$ das additive Inverse von r_g in R ist (dieses existiert, da R ein Ring ist). Man rechnet nach, dass die Addition und das Faltungsprodukt assoziativ sind und, dass die beiden Operationen distributiv sind.

(b) $R[G]$ ist kommutativ, falls sowohl R als auch G kommutativ sind: R ist auf natürliche Weise ein Unterring von $R[G]$, indem wir $r \in R$ als $r = r\, e_G$ auffassen. Ausserdem ist G auch eine Untergruppe von $R[G]$ (bezüglich Multiplikation in $R[G]$), indem wir $g = 1_R\, g$ schreiben, wobei wir mit 1_R das Einselement in R bezeichnen,. Dies zeigt, dass $R[G]$ genau dann kommutativ ist, wenn es G und R sind.

(c) Sei $e_G \neq g \in G$ mit n minimal, so dass $g^n = e_G$. Dann ist $1_R - g \in R[G]$ ein Nullteiler, da

$$(1_R - g)\cdot(1_R + g + g^2 + \cdots + g^{n-1}) = 1_R - g^n = 1 - 1 = 0 \in R[G].$$

(d) Angenommen 2 ist in R invertierbar. Wir schreiben $\mathbb{Z}/2\mathbb{Z}$ multiplikativ und nennen das neutrale Element e und den Erzeuger a. Wir definieren

$f : R\times R \to R[\mathbb{Z}/2\mathbb{Z}]$, $(r,s) \mapsto 2^{-1}r(e+a)+2^{-1}s(e-a) = 2^{-1}(r+s)e+2^{-1}(r-s)a$.

Dann gilt für $r, r', s, s' \in R$

$f(r+r', s+s') = 2^{-1}(r+r'+s+s')e+2^{-1}(r+r'-(s+s')a = f(r,s)+f(r',s')$

und

$$\begin{aligned} f(r,s)\cdot f(r',s') &= \big(2^{-1}r(e+a)+2^{-1}s(e-a)\big)\cdot\big(2^{-1}r'(e+a)+2^{-1}s'(e-a)\big) \\ &= 2^{-2}rr'(e+a)^2 + 2^{-2}ss'(e-a)^2 + 2^{-2}rs'(e+a)(e-a) + 2^{-2}sr'(e-a)(e+a) \\ &= 2^{-1}rr'(e+a) + 2^{-1}ss'(e-a) \\ &= f(rr', ss'), \end{aligned}$$

woraus folgt, dass f ein Ringhomomorphismus ist, da $f(1_R, 1_R) = 2^{-1} \cdot 2 \cdot 1_R e = 1_R\, e$. Ausserdem gilt $f(1_R, -1_R) = 1_R\, a$. Ist nun $r\, e + s\, a \in R[\mathbb{Z}/2\mathbb{Z}]$, so gilt $f(r+s, r-s) = f(r,r) + f(s,-s) = r\, e + s\, a$, woraus folgt, dass f surjektiv ist. Angenommen $f(r,s) = 2^{-1}r(e+a) + 2^{-1}s(e-a) = 1_R\, e$. Dann folgt direkt $r = s$ und dann $r = 1_R$, was die Injektivität von f beweist.

(e) Sei $f : G \to R^\times$ ein Gruppenhomomorphismus. Wir definieren $F : \mathbb{Z}[G] \to R$ durch $\sum_{g\in G} n_g\, g \mapsto \sum_{g\in G} n_g f(g)$.

Andererseits ist $H : \mathbb{Z}[G] \to R$ ein Ringhomomorphismus, so können wir H auf G einschränken und G ist eine (multikplikative) Untergruppe von $\mathbb{Z}[G]$ (siehe (b)). Daher induziert H einen Gruppenhomorphismus in die multiplikative Untergruppe der invertierbaren Elemente in R, d.h. einen Gruppenhomomorphismus $h := H_{|G} : G \to R^\times$.

Man prüft nach, dass die beiden Abbildungen wirklich Homomorphismen sind und invers zueinander.

(f) Sei $\mathbb{Z} = \langle a \rangle$. Wir definieren

$$f : R[X, Y] \to R[\mathbb{Z}], \quad X \mapsto a,\, Y \mapsto a^{-1}.$$

Dann ist f ein Ringhomomorphismus und surjektiv mit Kern $(1 - XY)$. Nach dem ersten Isomorphiesatz folgt $R[\mathbb{Z}] \cong R[X,Y]/(1-XY)$.

Sei $\mathbb{Z}/n\mathbb{Z} = \langle b \rangle$. Wir definieren

$$h : R[X] \to R[\mathbb{Z}/n\mathbb{Z}], \quad X \mapsto b.$$

Wie oben ist h ein Ringhomomorphismus und surjektiv mit Kern $(X^n - 1)$. Nach dem ersten Isomorphiesatz folgt $R[\mathbb{Z}/n\mathbb{Z}] \cong R[X]/(X^n - 1)$.