Problem Set 5 solutions

Problem 1. Let R be a commutative ring and I an ideal of R. Show that if R is noetherian the R/I is also noetherian.

Proof. There is an order preserving bijection

$$\{\text{ideals of } R \text{ that contain } I\} \longleftrightarrow \{\text{ideals of } R/I\}$$

that sends the ideal $J \supseteq I$ to J/I; its inverse is the map that sends each ideal in R/I to its preimage. Given this bijection, chains of ideals in R/I come from chains of ideals in R that contain J. Given an ascending chain

$$J_1/I \subseteq J_2/I \subseteq \cdots$$

of ideals in R/I, we have an ascending chain

$$J_1 \subseteq J_2 \subseteq \cdots$$

in R. Since R is noetherian, then this chain stops: there exists N such that $J_n = J_{n+1}$ for all $n \geqslant N$. Then $J_n/I = J_{n+1}/I$ for all $n \geqslant N$, and the original chain in R/I must also stop. □

Problem 2. Let R be a commutative ring with $1 \neq 0$. Show that

$$\operatorname{ann}_R(M \oplus N) = \operatorname{ann}_R(M) \cap \operatorname{ann}_R(N)$$

Proof.

$$\begin{aligned} r \in \operatorname{ann}_R(M \oplus N) &\iff r(m,n) = (0_M, 0_N) \text{ for all } (m,n) \in M \oplus N \\ &\iff (rm, rn) = (0_M, 0_N) \text{ for all } (m,n) \in M \oplus N \\ &\iff rm = 0_M \text{ and } rn = 0_N \text{ for all } m \in M, n \in N \\ &\iff r \in \operatorname{ann}_R(M) \cap \operatorname{ann}_R(N). \quad \square \end{aligned}$$

Problem 3. Let R be a domain and let M be an R-module. The torsion submodule of M is

$$\operatorname{Tor}(M) = \{m \in M \mid rm = 0 \text{ for some } r \in R \text{ with } r \neq 0\}.$$

Elements of $\operatorname{Tor}(M)$ are called the torsion elements of M, and the module M is called **torsion-free** if $\operatorname{Tor}(M) = 0$. You may take for granted that this is actually a submodule of M without proof.

a) Show that if M and N are R-modules, then $\operatorname{Tor}(M \oplus N) = \operatorname{Tor}(M) \oplus \operatorname{Tor}(N)$.

Proof. We argue by showing two containments. On the one hand, we have

$$\begin{aligned} \operatorname{Tor}(M \oplus N) &= \{(m,n) \in M \oplus N \mid r(m,n) = 0 \text{ for some } r \in R \setminus \{0\}\} \\ &= \{(m,n) \in M \oplus N \mid (rm, rn) = 0 \text{ for some } r \in R \setminus \{0\}\} \\ &\subseteq \operatorname{Tor}(M) \oplus \operatorname{Tor}(N) \end{aligned}$$

On the other hand, if $m \in \operatorname{Tor}(M)$ then there exists a nonzero $r \in R$ such that $rm = 0$, so $r(m,0) = 0$, and thus $(m,0) \in \operatorname{Tor}(M \oplus N)$. Similarly, if $n \in \operatorname{Tor}(N)$ then $rn = 0$ for some nonzero $r \in R$, and thus $r(0,n) = 0$, so $(0,n) \in \operatorname{Tor}(M \oplus N)$. Because $\operatorname{Tor}(M \oplus N)$ is a submodule and hence closed under taking sums, it follows that $(m,n) \in \operatorname{Tor}(M \oplus N)$ whenever $m \in \operatorname{Tor}(M)$ and $n \in \operatorname{Tor}(N)$. Equivalently $\operatorname{Tor}(M \oplus N) \subseteq \operatorname{Tor}(M) \oplus \operatorname{Tor}(N)$. Since we showed before that $\operatorname{Tor}(M) \oplus \operatorname{Tor}(N) \subseteq \operatorname{Tor}(M \oplus N)$, we conclude that $\operatorname{Tor}(M \oplus N) = \operatorname{Tor}(M) \oplus \operatorname{Tor}(N)$. □

b) Show that if $M \cong N$, then $\text{Tor}(M) \cong \text{Tor}(N)$.

Proof. Let $\phi : M \to N$ is an R-module isomorphism. We claim that $\text{Tor}(N) = \phi(\text{Tor}(M))$, and thus in particular $\text{Tor}(N) \cong \text{Tor}(M)$.

Given $n \in \text{Tor}(N)$, let $r \in R$ be a nonzero element such that $rn = 0$. Since ϕ is surjective, we can find some $m \in M$ such that $\phi(m) = n$. Notice that m is necessarily nonzero, since $\phi(0) = 0$. On the other hand, $\phi(rm) = r\phi(m) = rn = 0$, and since ϕ is injective, we conclude that $rm = 0$. Thus $n = \phi(m) \in \phi(\text{Tor}(M))$.

Conversely, if $n \in \phi(\text{Tor}(M))$, then $n = \phi(m)$ for some $M \in \text{Tor}(M)$. Then we can find some nonzero $r \in R$ such that $rm = 0$, and thus $rn = r\phi(m) = \phi(rm) = \phi(0) = 0$. We conclude that $n \in \text{Tor}(N)$. ☐

c) Show that if M is a free R-module then $\text{Tor}(M) = 0$.

Proof. If $M = 0$, since $\text{Tor}(M) \subseteq M$ and 0 is a torsion element it follows that $\text{Tor}(M) = 0$.

If $M \neq 0$ is free, then there exists a basis B for M. Consider a nonzero $m \in M$. Then

$$m = r_1 b_1 + \cdots + r_n b_n$$

for some elements $b_i \in B$ and $0 \neq r_i \in R$. Suppose $rm = 0$ for some $r \in R$. Then

$$\sum_{i=1}^{n} (rr_i) b_i,$$

and since B is linearly independent we deduce that $rr_i = 0$ for $1 \leqslant i \leqslant n$. Since R is a domain, it follows that either $r = 0$ or $r_i = 0$ for all $1 \leqslant i \leqslant n$. But $m \neq 0$, so $r_i \neq 0$ for some i, so we conclude that $r = 0$. Hence any nonzero $m \in M$ is not a torsion element, and $\text{Tor}(M) = 0$. ☐

d) Show that if $I \neq (0)$ is an ideal of R then $\text{Tor}(R/I) = R/I$.

Proof. Here we consider R/I *as an R-module*. Let $r + I \in R/I$ and let $0 \neq j \in I$. Then $j(r+I) = jr + I = 0 + I$, so $r + I \in \text{Tor}(R/I)$. Since $r + I \in R/I$ was arbitrary, we conclude that $R/I \subseteq \text{Tor}(R/I)$. But $\text{Tor}(R/I)$ is by definition a subset of R/I, and thus $R/I = \text{Tor}(R/I)$. ☐

e) Suppose that R is a PID, and that M is a finitely generated R-module. Show that M is a torsion-free R-module if and only if M is a free R-module.

Proof. By the classification theorem for modules over PIDs, $M \cong R^r \oplus R/(d_1) \oplus \cdots \oplus R/(d_k)$, where $d_1, \ldots d_k$ are the invariant factors of M. Then

$$\begin{aligned}
0 &= \text{Tor}(M) && \text{since } M \text{ is torsion-free} \\
&\cong \text{Tor}\left(R^r \oplus R/(d_1) \oplus \cdots \oplus R/(d_k)\right) && \text{by e)} \\
&\cong \text{Tor}(R^r) \oplus \text{Tor}(R/(d_1)) \oplus \cdots \oplus \text{Tor}(R/(d_k)) && \text{by a)} \\
&= 0 \oplus R/(d_1) \oplus \cdots \oplus R/(d_k) && \text{by b) and d).}
\end{aligned}$$

Thus $\text{Tor}(M) = 0$ if and only if $k = 0$, which is equivalent to $M \cong R^r$. We conclude that $\text{Tor}(M) = 0$ if and only if M is a free R-module. ☐

Problem 4. Consider the matrix

$$A = \begin{bmatrix} 1 & 6 & 5 & 2 \\ 2 & 1 & -1 & 0 \\ 3 & 0 & 3 & 0 \end{bmatrix} \in \mathrm{M}_{3,4}(\mathbb{Z}).$$

Determine the simplest representative in the isomorphism class of the $\mathbb{Z}$-module presented by A.

Proof. Starting from the matrix A, first do three column operations, adding (-6) times the first column to the second column, adding (-5) times the first column to the third column, and adding (-2) time the first column to the fourth column; this gives the matrix $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & -11 & -11 & -4 \\ 3 & -18 & -12 & -6 \end{bmatrix}$. Next do two row operations, adding (-2) times row 1 to row 2, and adding (-3) times row 1 to row 3, resulting in the matrix $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -11 & -11 & -4 \\ 0 & -18 & -12 & -6 \end{bmatrix}$. Next add (-1) times column 2 to column 3, to get $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -11 & 0 & -4 \\ 0 & -18 & 6 & -6 \end{bmatrix}$. Now add (-3) times column 4 to column 2, which gives $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -4 \\ 0 & 0 & 6 & -6 \end{bmatrix}$. Finally, doing two more column operations, adding 4 times column 2 to column 4, and then adding 1 times column 3 to column 4, gives $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 6 & 0 \end{bmatrix}$. Lastly, consider the matrix A' obtained by eliminating the column of zeroes, as well as the columns corresponding the the elementary basis vectors in the previous matrix and the rows where they have 1's. This gives $A' = (6)$.

By a theorem from class, the module presented by A is isomorphic to the module presented by A'. The latter is, by definition, $\mathbb{Z}/\operatorname{im}(t_{A'})$ where $t_{A'} : \mathbb{Z} \to \mathbb{Z}$ is the map $x \mapsto 6x$. This gives that $\operatorname{im}(t_{A'}) = (6)$ and the module presented by A' is $\mathbb{Z}/6$. □

Problem 5. Let R be a PID and let M be a finitely generated R-module.

a) Determine a generator for the principal ideal $\operatorname{ann}_R(M)$ in terms of the invariant factors and the free rank of M.

Proof. First, we claim that $\operatorname{ann}_R(R/(d)) = (d)$. If $r \in (d)$ then $r(x + (d)) = rx + (d) = 0 + (d)$ so $(d) \subseteq \operatorname{ann}_R(R/(d))$. Conversely, if $r \in \operatorname{ann}_R(R/(d))$ then $r(1 + (d)) = 0 + (d)$, thus $r \in (d)$. This shows that $\operatorname{ann}_R(R/(d)) = (d)$, as claimed.

We claim that if the free rank of M is r and the invariant factors of M are $d_1 \mid d_2 \mid \ldots \mid d_k$ then

$$\operatorname{ann}_R(M) = \begin{cases} (0) & \text{if } r > 0 \\ (d_k) & \text{if } r = 0. \end{cases} \quad \square$$

Notice that $\operatorname{ann}_R(R) = (0)$, since the only element that kills 1 is 0. By Problem 6 we have

$$\operatorname{ann}_R\left(R^r \oplus R/(d_1) \oplus \cdots \oplus R/(d_k)\right) = \begin{cases} \operatorname{ann}_R(R) \cap \operatorname{ann}_R(R/(d_1)) \cap \ldots \cap \operatorname{ann}_R(R/(d_k)), r > 0 \\ \operatorname{ann}_R(R/(d_1)) \cap \ldots \cap \operatorname{ann}_R(R/(d_k)), r = 0 \end{cases}$$

$$= \begin{cases} (0) \cap (d_1) \cap \ldots \cap (d_k) & \text{if } r > 0 \\ (d_1) \cap \ldots \cap (d_k) & \text{if } r = 0 \end{cases} = \begin{cases} (0) & \text{if } r > 0 \\ (d_k) & \text{if } r = 0 \end{cases}$$

b) Determine a generator for the principal ideal $\operatorname{ann}_R(M)$ in terms of the elementary divisors and the free rank of M.

Proof. We will show if the free rank of M is r and the elementary divisors are $p_1^{e_1}, \dots, p_s^{e_s}$ then

$$\operatorname{ann}_R(M) = \begin{cases} (0) & \text{if } r > 0 \\ (\mathrm{lcm}(\mathrm{p}_1^{\mathrm{e}_1}, \dots, \mathrm{p}_s^{\mathrm{e}_s})) & \text{if } r = 0. \end{cases} \quad \square$$

As in a), we have

$$\operatorname{ann}_R\left(R^r \oplus R/(p_1^{e_1}) \oplus \cdots \oplus R/(p_s^{e_s})\right) = \begin{cases} (0) \cap (p_1^{e_1}) \cap \ldots \cap (p_s^{e_s}) & \text{if } r > 0 \\ (p_1^{e_1}) \cap \ldots \cap (p_s^{e_s}) & \text{if } r = 0. \end{cases}$$

The claim follows if we show that $(p_1^{e_1}) \cap \ldots \cap (p_s^{e_s}) = (\mathrm{lcm}(\mathrm{p}_1^{\mathrm{e}_1}, \dots, \mathrm{p}_s^{\mathrm{e}_s}))$. Indeed:

($\subseteq$) If $r \in (p_1^{e_1}) \cap \ldots \cap (p_s^{e_s})$, then $r \in (p_i^{e_i})$ for all i, and in particular $p_i^{e_i} | r$ for all i. Therefore, $\mathrm{lcm}(\mathrm{p}_1^{\mathrm{e}_1}, \dots, \mathrm{p}_s^{\mathrm{e}_s})|\mathrm{r}$, and thus $r \in (\mathrm{lcm}(\mathrm{p}_1^{\mathrm{e}_1}, \dots, \mathrm{p}_s^{\mathrm{e}_s}))$.

($\supseteq$) Suppose that $r \in (\mathrm{lcm}(\mathrm{p}_1^{\mathrm{e}_1}, \dots, \mathrm{p}_s^{\mathrm{e}_s}))$. Thus $p_i^{e_i} | \mathrm{lcm}(\mathrm{p}_1^{\mathrm{e}_1}, \dots, \mathrm{p}_s^{\mathrm{e}_s})|\mathrm{r}$, which by transitivity implies that $p_i^{e_i} | r$, and $r \in (p_i^{e_i})$ for all i.

Problem 6. Consider the matrix $A = \begin{bmatrix} x & 1 & 0 \\ 1 & x & -3 \\ 0 & 0 & x-1 \end{bmatrix} \in \mathrm{M}_{3,3}(R)$, where $R = \mathbb{Q}[x]$ is a ED.

a) Determine the Smith normal form for A.

Solution. $\begin{pmatrix} x & 1 & 0 \\ 1 & x & -3 \\ 0 & 0 & x-1 \end{pmatrix} \xrightarrow{(1)} \begin{pmatrix} 1 & x & 0 \\ x & 1 & -3 \\ 0 & 0 & x-1 \end{pmatrix} \xrightarrow{(2)} \begin{pmatrix} 1 & 0 & 0 \\ x & -x^2+1 & -3 \\ 0 & 0 & x-1 \end{pmatrix}$

$\xrightarrow{(3)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -x^2+1 & -3 \\ 0 & 0 & x-1 \end{pmatrix} \xrightarrow{(4)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & -x^2+1 \\ 0 & x-1 & 0 \end{pmatrix}$

$\xrightarrow{(5)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & x-1 & -\frac{1}{3}(x^2-1)(x-1) \end{pmatrix} \xrightarrow{(6)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & -\frac{1}{3}(x^2-1)(x-1) \end{pmatrix}$

$\xrightarrow{(7)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (x^2-1)(x-1) \end{pmatrix}$,

where

(1) is a permutation swapping columns 1 and 2,
(2) adds $-x$ times column 1 to column 2,
(3) adds $-x$ times row 1 to row 2,
(4) is a permutation swapping columns 2 and 3,
(5) adds $-\frac{1}{3}(x^2-1)$ times column 2 to column 3,
(6) adds $-\frac{1}{3}(-x+1)$ times row 2 to row 3,
(7) multiplies row 2 by the unit $-\frac{1}{3}$ in $\mathbb{R}$ and multiplies row 3 by the unit -3 in $\mathbb{R}$. $\square$

b) Determine the representatives in the isomorphism class of the module presented by A which are written in invariant factor form and in elementary divisor form.

Solution. Since the unique invariant factor of A is $(x^2-1)(x-1)$ from the SNF, the invariant factor decomposition of the $\mathbb{R}[x]$-module presented by A is

$$\mathbb{R}[x]/((x^2-1)(x-1)).$$

The elementary divisor decomposition is obtained from the above by using the CRT. It is the last module in the following isomorphism

$$\mathbb{R}[x]/((x^2-1)(x-1)) = \mathbb{R}[x]/((x+1)(x-1)^2) \cong \mathbb{R}[x]/(x+1) \oplus \mathbb{R}[x]/((x-1)^2). \quad \square$$