Rings and modules - Repetition exam

Solved on Friday 24.11

Problem 1. Find the Smith normal form over the integers $\mathbb{Z}$ for the matrix $\begin{pmatrix} 2 & 4 & 2 \\ 2 & 4 & 6 \\ 3 & 5 & 7 \end{pmatrix}$.

Solution. We perform the following row and column operations

$$\begin{pmatrix} 2 & 4 & 2 \\ 2 & 4 & 6 \\ 3 & 5 & 7 \end{pmatrix} \overset{R_3 \to R_3 - R_2}{\longrightarrow} \begin{pmatrix} 2 & 4 & 2 \\ 2 & 4 & 6 \\ 1 & 1 & 1 \end{pmatrix} \overset{R_1 \leftrightarrow R_3}{\longrightarrow} \begin{pmatrix} 1 & 1 & 1 \\ 2 & 4 & 6 \\ 2 & 4 & 2 \end{pmatrix} \underset{C_3 \to C_3 - C_1}{\overset{C_2 \to C_2 - C_1}{\longrightarrow}} \begin{pmatrix} 1 & 0 & 0 \\ 2 & 2 & 4 \\ 2 & 2 & 0 \end{pmatrix} \underset{R_3 \to R_3 - 2R_1}{\overset{R_2 \to R_2 - 2R_1}{\longrightarrow}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 4 \\ 0 & 2 & 0 \end{pmatrix} \overset{C_3 \to C_3 - 2C_2}{\longrightarrow}$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 2 & -4 \end{pmatrix} \overset{R_3 \to R_3 - R_2}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -4 \end{pmatrix} \overset{R_3 \to -R_3}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}.$$

Hence the Smith normal form of the given matrix is $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}$.

Problem 2. Consider the ring $R = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$, where $\mathbb{R}$ denotes the real numbers, and the subset $I = \left\{ \begin{pmatrix} 0 & 0 \\ b & 0 \end{pmatrix} \mid b \in \mathbb{R} \right\}$.

(a) Show that I is an ideal in R. Is the ring R commutative, artinian, noetherian, semisimple? Is the ring R/I commutative, artinian, noetherian, semisimple?

(b) Find two maximal ideals m_1, m_2 in R, such that $m_1 \cap m_2 = I$.

(c) Show that there are no other maximal ideals in R.

(d) Find two simple R-modules which are not isomorphic.

Solution.

(a) We have that $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in I$ and so $I \neq \varnothing$. Let $\begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ y & 0 \end{pmatrix} \in I$ and $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in R$. We have that

$$\begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ y & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ x + y & 0 \end{pmatrix} \in R,$$

and

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ cx & 0 \end{pmatrix} \in I,$$

and also

$$\begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ xa & 0 \end{pmatrix} \in I,$$

showing indeed that I is a (two-sided) ideal of R.

The ring R is clearly not commutative as

$$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix} = \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix} \neq \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix} = \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}.$$

Next notice that R is a 3-dimensional $\mathbb{R}$-algebra (since it is a vector space over $\mathbb{R}$ and the matrix multiplication of R is compatible with the vector space structure). Therefore all left or right submodules of R are in particular subspaces of R of dimension at most 3. Therefore, in every increasing or decreasing chain of left or right submodules of R, there can be at most three proper containments. It follows that every such chain stabilizes and so R is both left and right artinian and noetherian. Hence R is artinian and noetherian.

Next we have that the ring R is not semisimple since the ideal I is non-zero but is nilpotent. Indeed, for $X = \begin{pmatrix}0 & 0\\ x & 0\end{pmatrix} \in I$ we have

$$X^2 = \begin{pmatrix}0 & 0\\ x & 0\end{pmatrix}\begin{pmatrix}0 & 0\\ x & 0\end{pmatrix} = \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix},$$

and so $I^2 = (0)$.

Now we move on to R/I. Clearly we have

$$R/I \cong \left\{\begin{pmatrix}a & 0\\ 0 & c\end{pmatrix} \mid a, c \in \mathbb{R}\right\} \cong \mathbb{R}\times\mathbb{R},$$

where the last isomorphism is the map which sends $\begin{pmatrix}a & 0\\ 0 & c\end{pmatrix}$ to (a, c). Then for $(a_1, c_1), (a_2, c_2) \in \mathbb{R}\times\mathbb{R}$ we have

$$(a_1, c_1)(a_2, c_2) = (a_1a_2, c_1c_2) = (a_2a_1, c_2c_1) = (a_2, c_2)(a_1, c_1),$$

and so R/I is commutative. By the Wedderburn–Artin theorem we have that $\mathbb{R}\times\mathbb{R}$ is a semisimple ring, and so R/I is semisimple. In particular, and since $\mathbb{R}$ is a field, we have that the only ideals of $\mathbb{R}\times\mathbb{R}$ are $(0)\times(0)$, $(0)\times\mathbb{R}$, $\mathbb{R}\times(0)$ and $\mathbb{R}\times\mathbb{R}$. Since there are only finitely many ideals, there can be no infinite strictly decreasing or increasing chain of ideals of $\mathbb{R}\times\mathbb{R}$ and hence $\mathbb{R}\times\mathbb{R}$ is both artinian and notherian. We conclude that R/I is both artinian and noetherian too.

(b) It is straightforward to check that the sets m_1 and m_2 where

$$m_1 = \left\{\begin{pmatrix}a & 0\\ b & 0\end{pmatrix} \mid a, b \in \mathbb{R}\right\} \text{ and } m_2 = \left\{\begin{pmatrix}0 & 0\\ b & c\end{pmatrix} \mid b, c \in \mathbb{R}\right\}$$

are two-sided ideals of R. Clearly also $m_1 \cap m_2 = I$. It remains to show that they are maximal ideals. To show that m_1 is a maximal ideal, let J be a two-sided ideal of R with $m_1 \subsetneq J \subseteq R$ and it is enough to show that $J = R$. Since $J \neq m_1$, there exists a matrix $\begin{pmatrix}a & 0\\ b & c\end{pmatrix} \in J$ with $c \neq 0$. Then

$$\begin{pmatrix}0 & 0\\ 0 & c^{-1}\end{pmatrix}\begin{pmatrix}a & 0\\ b & c\end{pmatrix} = \begin{pmatrix}0 & 0\\ c^{-1}b & 1\end{pmatrix} \in J$$

and since $m_1 \subseteq J$, we also have that $\begin{pmatrix}-1 & 0\\ c^{-1}b & 0\end{pmatrix} \in J$. Then

$$\begin{pmatrix}0 & 0\\ c^{-1}b & 1\end{pmatrix} - \begin{pmatrix}-1 & 0\\ c^{-1}b & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \in J,$$

and since the identity element of R is in J, we have $J = R$. This shows that m_1 is a maximal ideal and similarly one may show that m_2 is a maximal ideal as well.

(c) Let m be a maximal ideal of R. Then either $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in m$ or $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \notin m$.

Assume first that $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in m$. Then the ideal generated by $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is just m_1 and so $m_1 \subseteq m$. By maximality of m_1, and since $m \neq R$ as it is itself maximal, we conclude that $m_1 = m$ in this case.

Assume now that $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \notin m$. Let $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in m$. We claim that $a = 0$. Indeed, otherwise we have that

$$\begin{pmatrix} a^{-1} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in m,$$

contradicting our assumption. Hence all matrices in m are of the form $\begin{pmatrix} 0 & 0 \\ b & c \end{pmatrix}$ with $b, c \in \mathbb{R}$. Therefore $m \subseteq m_2$. But m is maximal and $m_2 \neq R$ since m_2 is also maximal, and so $m = m_2$ in this case.

Hence we have shown that any maximal ideal of R is equal to one of m_1 or m_2.

(d) We have that I is a submodule of R which is 1-dimensional as an $\mathbb{R}$-vector space. Hence its only submodules are 0 and I and so I is a simple left R-module. Similarly, we may see that

$$S = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & c \end{pmatrix} \mid c \in \mathbb{R} \right\}$$

is a simple left R-module. Moreover, we have that $I^2 = 0$ while $S^2 \neq 0$ since $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Therefore I and S are not isomorphic.

Problem 3. (a) For any unital ring R and any ideal I in R, show that the left modules over R/I are exactly the left modules M such that $IM = 0$.

(b) Let $R = F[X]$ for a field F and let $I = (X^2)$. Show that for an R/I-module M, the following three statements are equivalent:

(i) M is finitely generated as an R-module.

(ii) M is finitely generated as an R/I-module.

(iii) M is finite dimensional as an F-vector space (= F-module).

(c) Classify all finitely generated modules over $F[X]/(X^2)$ (up to isomorphism).

Solution.

(a) First let M be an R/I-module. Then M becomes an R-module by defining $rm = (r + I)m$ for any $r \in R$ and $m \in M$ (the fact that the module axioms hold is inherited from the fact that they hold for M as an R/I-module). Hence if $a \in I$, then

$$am = (a + I)m = (0 + I)m = 0,$$

showing that $IM = 0$.

Now let M be an R-module such that $IM = 0$. We claim that M becomes an R/I-module via $(r+I)m = rm$ for any $r \in R$ and $m \in M$. The only thing needed to do is to show that this is well-defined, since then again the module axioms hold because they hold for M as an R-module. Hence assume that $r+I = s+I$ so that $r - s \in I$. Then $(r - s)m = 0$ since $(r - s)m \in IM = 0$. Therefore $rm - sm = 0$ or $rm = sm$ and so

$$(r + I)m = rm = sm = (s + I)m,$$

as required.

(b) Assume first that (iii) holds. Let $m_1, \ldots, m_k$ be an F-basis of M. Then for any $m \in M$ there exist $f_1, \ldots, f_k \in F$ such that

$$m = f_1 m_1 + \cdots + f_k m_k.$$

Notice that $f_1, \ldots, f_k \in F \subseteq F[X]$ and moreover each f_i is in its own equivalence class in $F[X]/(X^2)$ since $f_i - f_j \notin (X^2)$. Therefore, we also have that

$$m = f_1 m_1 + \cdots + f_k m_k = (f_1 + I)m_1 + \cdots + (f_k + I)m_k,$$

showing that M is finitely generated as a R/I-module and so (ii) holds.

Now assume that (ii) holds. Then there exist $x_1, \ldots, x_n \in M$ such that for every $m \in M$ there exist $p_1(X) + I, \ldots, p_n(X) + I \in R/I$ such that

$$m = (p_1(X) + I)x_1 + \cdots + (p_n(X) + I)x_n.$$

But by part (a), we have that M is also an R-module with multiplication such that

$$m = p_1(X)x_1 + \cdots + p_n(X)x_n.$$

This shows that M is finitely generated as an R-module as well and so (i) holds.

Finally we assume that (i) holds and we show that (iii) holds. Let $\{y_1, \ldots, y_l\}$ be a set that generates M as an R-module. Then for every $m \in M$ there exist $q_1(X), \ldots, q_l(X) \in R = F[X]$ such that

$$m = q_1(X)y_1 + \cdots + q_l(X)y_l. \tag{1}$$

If $q(X) = a_0 + a_1 X + \cdots + a_s X^s$, then, since $(X^2)M = 0$ by part (a) (as M is an $F[X]/(X^2)$-module), we obtain for any $m' \in M$ that

$$q(X)m' = (a_0 + a_1 X)m'.$$

Let $q_i(X) = a_{i0} + a_{i1}X + \cdots$ with coefficients in F. Then (1) becomes

$$m = (a_{10} + a_{11}X)y_1 + \cdots + (a_{l0} + a_{l1}X)y_l = a_{10}y_1 + \cdots + a_{l0}y_l + a_{10}(Xy_1) + \cdots + a_{l0}(Xy_l),$$

and so $y_1, \ldots, y_l, Xy_1, \ldots, Xy_l$ generate M as an F-module. Therefore M is finitely generated as an F-module and hence a finite dimensional F-vector space, showing (iii).

(c) We claim that $F[X]/(X^2)$ is a PID. Indeed, let J be an ideal of $F[X]/(X^2)$. If there exists an element of the form $f + (X^2) \in J$ with $f \in F \neq \{0\}$, then $f + (X^2)$ is a unit and so $J = F[X]/(X^2)$. If no such element exists, then all elements of J are of the form $aX + (X^2)$ for some $a \in F$ (since higher powers of X vanish in $F[X]/(X^2)$). But then $(a^{-1} + (X^2))(aX + (X^2)) = X + (X^2) \in J$, and so $J = (X + (X^2))$. Therefore indeed $F[X]/(X^2)$ is a PID.

Let M be a finitely generated $F[X]/(X^2)$ module. Since $F[X]/(X^2)$ is a PID, we have by the structure theorem for finitely generated modules over a PID that

$$M \cong (R/I)^s \oplus \frac{R/I}{(p_1(X) + (X^2))} \oplus \cdots \oplus \frac{R/I}{(p_u(X) + (X^2))} \tag{2}$$

where $s \geq 0$ is an integer and $p_1(X) + (X^2), \ldots, p_u(X) + (X^2)$ are nonzero nonunits such that $p_1(X) + (X^2) \mid \cdots \mid p_u(X) + (X^2)$. It follows from our classification of ideals of $F[X]/(X^2)$ in the first paragraph of this part that each $(p_i(X) + (X^2)) = (X + (X^2))$. Therefore, we have that

$$\frac{R/I}{(p_i(X) + (X^2))} = \frac{R/I}{(X + (X^2))} = \frac{\frac{F[X]}{(X^2)}}{(X + (X^2))} \cong \frac{F[X]}{(X)},$$

where the last isomorphism follows since $(X^2) \subseteq (X)$. Since $\frac{F[X]}{(X)} \cong F$, we conclude that each direct summand

$$\frac{R/I}{(p_i(X) + (X^2))}$$

in (2) is isomorphic to F. Replacing this in (2) we obtain that

$$M \cong (R/I)^s \oplus F^u$$

for some integers $s, u \geq 0$. Hence any finitely generated R/I-module has this form up to isomorphism.

Problem 4. Let R be a unital ring, and let M be a left R-module.

(a) Show that if M is noetherian, then all submodules of M are finitely generated.

(b) Show that if M is both noetherian and artinian, then there is a finite sequence of submodules

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_{n-1} \supseteq M_n = 0,$$

such that M_i/M_{i+1} is a simple R-module, for $i = 0, \ldots, n-1$.

Give an example to show that such a finite sequence does not necessarily exist if M is only noetherian (and not artinian).

Solution.

(a) Suppose to a contradiction that M is noetherian but there exists a submodule N of M which is not finitely generated. Let $n_1 \in N$. Then $(n_1) \neq N$, and so there exists $n_2 \in N \setminus (n_1)$. Then $(n_1) \neq (n_1, n_2)$ since $n_2 \notin (n_1)$. Moreover, we also have $(n_1, n_2) \neq N$ since N is not finitely generated, and so there exists $n_3 \in N \setminus (n_1, n_2)$. Then $(n_1, n_2) \neq (n_1, n_2, n_3) \neq N$ and continuing this way we may build an infinite ascending chain of submodules of M

$$(n_1) \subsetneq (n_1, n_2) \subsetneq (n_1, n_2, n_3) \subsetneq \cdots .$$

But this contradicts the assumption that M is noetherian. Hence all submodules of M are finitely generated.

(b) Since M is noetherian, there exists a maximal element in the collection of all submodules of M, say M_1. In other words, M_1 is a submodule of M such that there exists no submodule N of M with $M_1 \subsetneq N \subsetneq M$. By the correspondence theorem, every submodule of M/M_1 is of the form U/M_1 where U is a submodule of M containing M_1. By maximality of M_1 we have that $U = M$ or $U = M_1$. If $U = M$, then $U/M_1 = M/M_1$, while if $U = M_1$, then $U/M_1 = M_1/M_1 = 0$. Therefore, the only submodules of M/M_1 are M/M_1 and 0 and so M/M_1 is simple.

Now we may define M_2 as a maximal submodule of M contained in M_1, so that M_1/M_2 is also simple. Continuing this way we obtain a descending chain of submodules

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots ,$$

such that M_i/M_{i+1} is simple. But such a chain must stabilize since M is artinian and so the claim follows.

For an example where such a property does not hold, let $R = \mathbb{Z}$. Then $\mathbb{Z}$ is noetherian but not artinian. If we consider the chain

$$(2) \supseteq (2^2) \supseteq (2^3) \supseteq \cdots . \tag{3}$$

We claim that $(2^i)/(2^{i+1})$ is simple for any $i \geq 1$. Indeed, it is enough to show that there exists no ideal strictly between (2^i) and (2^{i+1}). If

$$(2^i) \supseteq I \supseteq (2^{i+1}),$$

then, since $\mathbb{Z}$ is a PID, we obtain that $I = (a)$ for some $a \in \mathbb{Z}$ and so

$$(2^i) \supseteq (a) \supseteq (2^{i+1}).$$

Then $2^i \mid a \mid 2^{i+1}$ and so $a = 2^i$ or $a = 2^{i+1}$. Hence indeed $(2^i)/(2^{i+1})$ is simple for any $i \geq 1$. But the chain of submodules (3) never terminates.