Rings, Modules and Linear Algebra — Exam solutions

(1) (i) **[similar examples seen]**

(a) The characteristic polynomial of A is the determinant of the matrix on the left below. The matrix on the right is obtained by adding $t-1$ times the second row to the first row and $t-1$ times the fourth row to the third row, so it has the same determinant.

$$\begin{pmatrix} t-1 & -1 & -1 & -1 \\ -1 & t-1 & -1 & -1 \\ 0 & 0 & t-1 & -1 \\ 0 & 0 & -1 & t-1 \end{pmatrix} \to \begin{pmatrix} 0 & t^2-2t & -t & -t \\ -1 & t-1 & -1 & -1 \\ 0 & 0 & 0 & t^2-2t \\ 0 & 0 & -1 & t-1 \end{pmatrix}$$

We now expand the determinant repeatedly along the first column to get

$$\begin{vmatrix} t^2-2t & -t & -t \\ 0 & 0 & t^2-2t \\ 0 & -1 & t-1 \end{vmatrix} = (t^2-2t) \begin{vmatrix} 0 & t^2-2t \\ -1 & t-1 \end{vmatrix} = (t^2-2t)^2 = t^2(t-2)^2.\mathbf{[4]}$$

(b) The reduced echelon form of A is clearly given by

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

so $\text{rank}(A) = 2$ **[2]**. Below we display the row-reduction of $A - 2I$:

$$\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & 1 & 1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

This makes it clear that $\text{rank}(A - 2I) = 3$ **[2]**.

(c) By looking at the characteristic polynomial, we see that M_A is a direct sum of modules of the form $B(0,k)$ or $B(2,k)$, with $1 \le k \le 2$. Each $B(0,k)$ contributes t^k to the characteristic polynomial, and each $B(2,k)$ contributes $(t-2)^k$. The number of blocks of eigenvalue 0 is $4 - \text{rank}(A) = 2$, and the number of blocks with eigenvalue 1 is $4 - \text{rank}(A-2I) = 1$. The only possibility is to have $M_A = B(0,1) \oplus B(0,1) \oplus B(2,2)$ **[4]**.

(ii) **[similar examples seen]**We first observe that $1296 = 2^4 3^4$, so M must be a direct sum of groups of the form $\mathbb{Z}_{2^j}$ or $\mathbb{Z}_{3^k}$, with $1 \le j, k \le 4$ **[2]**. As $18m = 2^1 3^2 m = 0$ for all $m \in M$, we must in fact have $j = 1$ and $1 \le k \le 2$, so the possible building blocks are $\mathbb{Z}_2$, $\mathbb{Z}_3$ and $\mathbb{Z}_9$ **[2]**. Thus, the 2-primary part must be $(\mathbb{Z}_2)^4$, and the 3-primary part could be $(\mathbb{Z}_9)^2$ or $(\mathbb{Z}_3)^2 \oplus \mathbb{Z}_9$ or $(\mathbb{Z}_3)^4$. Thus, there are thus 3 possibilities for M:

- $(\mathbb{Z}_2)^4 \oplus (\mathbb{Z}_9)^2$ **[1]**
- $(\mathbb{Z}_2)^4 \oplus (\mathbb{Z}_3)^2 \oplus \mathbb{Z}_9$ **[1]**
- $(\mathbb{Z}_2)^4 \oplus (\mathbb{Z}_3)^4$ **[1]**

(iii) **[The case $\lambda = 1$ was on a problem sheet]**

I claim that

$$A^n = \begin{pmatrix} \lambda^n & n\lambda^{n-1} \\ 0 & \lambda^n \end{pmatrix}$$

for all $n \ge 0$. Indeed, this is clear when $n = 0$, and if it holds for $n = k$ we have

$$A^{k+1} = AA^k = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} \lambda^k & k\lambda^{k-1} \\ 0 & \lambda^k \end{pmatrix} = \begin{pmatrix} \lambda^{k+1} & (k+1)\lambda^k \\ 0 & \lambda^{k+1} \end{pmatrix}$$

so it also holds for $n = k + 1$. It therefore holds for all k by induction **[3]**. It follows that

$$\begin{aligned} f(A) &= \sum_i a_i \begin{pmatrix} \lambda^i & i\lambda^{i-1} \\ 0 & \lambda^i \end{pmatrix} \\ &= \begin{pmatrix} \sum_i a_i \lambda^i & \sum_i i a_i \lambda^{i-1} \\ 0 & \sum_i a_i \lambda^i \end{pmatrix} \\ &= \begin{pmatrix} f(\lambda) & f'(\lambda) \\ 0 & f(\lambda) \end{pmatrix} \, \textbf{[3]}. \end{aligned}$$

(2) (i) **[similar examples seen]**
We can simplify B by row and column operations as follows:

$$\begin{pmatrix} 200 & 100 & 108 \\ 36 & 0 & 72 \\ 0 & 0 & 36 \end{pmatrix} \xrightarrow{1} \begin{pmatrix} 0 & 100 & 8 \\ 36 & 0 & 72 \\ 0 & 0 & 36 \end{pmatrix} \xrightarrow{2} \begin{pmatrix} 0 & 100 & 8 \\ 36 & -900 & 0 \\ 0 & -400 & 4 \end{pmatrix} \xrightarrow{3}$$

$$\begin{pmatrix} 0 & 900 & 0 \\ 36 & -900 & 0 \\ 0 & -400 & 4 \end{pmatrix} \xrightarrow{4} \begin{pmatrix} 0 & 900 & 0 \\ 36 & 0 & 0 \\ 0 & 0 & 4 \end{pmatrix} \xrightarrow{5} \begin{pmatrix} 4 & 0 & 0 \\ 0 & 36 & 0 \\ 0 & 0 & 900 \end{pmatrix}.$$

(In step 1 we subtracted C_2 from C_3, and $2C_2$ from C_1. In step 2 we subtracted $9R_1$ from R_2, and $4R_1$ from R_3. In step 3 we subtracted $2R_3$ from R_1, and in step 4 we added $25C_1 + 100C_3$ to C_2. Finally, in step 5 we permuted the rows and columns in an obvious way.) **[6]** [**3 marks will be awarded for a broadly correct method, with one mark deducted from this if the answer is not in normal form. The remaining 3 marks are for accuracy; one mark will be deducted for each error.**]
This shows that $\mathbb{Z}^3/N \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_{36} \oplus \mathbb{Z}_{900}$ **[2]**.

(ii) **[similar examples seen]**We can apply column operations as follows:

$$\begin{pmatrix} a & 1 & 0 & 0 \\ 0 & b & 1 & 0 \\ 0 & 0 & c & 1 \\ 0 & 0 & 0 & d \end{pmatrix} \to \begin{pmatrix} 0 & 1 & 0 & 0 \\ -ab & b & 1 & 0 \\ 0 & 0 & c & 1 \\ 0 & 0 & 0 & d \end{pmatrix} \to \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ abc & -bc & c & 1 \\ 0 & 0 & 0 & d \end{pmatrix}$$

$$\to \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -abcd & bcd & -cd & d \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ bcd & -cd & d & -abcd \end{pmatrix} \textbf{[3]}$$

We then apply row operations as follows

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ bcd & -cd & d & -abcd \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -abcd \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & abcd \end{pmatrix}.\textbf{[2]}$$

We conclude that $R^4/M \simeq R/1 \oplus R/1 \oplus R/1 \oplus R/abcd = R/abcd$, so R is cyclic and we can take $x = abcd$. **[3]**

(iii) [**There is one similar example in the lecture notes**] Put $w_1 = u_1 - u_2 = (1,1,0)$ and $w_2 = u_2 - u_3 = (0,2,2)$ and $w_3 = u_3 = (0,0,4)$ **[3]**. These give a new basis for L. If we put

$$\begin{aligned} d_1 &= 1 & v_1 &= (1,1,0) \\ d_2 &= 2 & v_2 &= (0,1,1) \\ d_3 &= 4 & v_3 &= (0,0,1)\textbf{[3]} \end{aligned}$$

then clearly $w_i = d_i v_i$ and $\{v_1, v_2, v_3\}$ is a basis for $\mathbb{Z}^3$ over $\mathbb{Z}$ **[3]**.

(3) (i) **[bookwork]**
As M is finitely generated, there is a list $m_1, \dots, m_d$ of elements of M such that an arbitrary element $m \in M$ can be written in the form $u_1 m_1 + \dots + u_d m_d$ [**1**]. Define $\phi\colon R^d \to M$ by $\phi(u_1, \dots, u_d) = u_1 m_1 + \dots + u_d m_d$; this is clearly a surjective homomorphism [**1**]. Put $L = \{u \in R^d \mid \phi(u) \in N\}$ [**1**]. I claim that this is a submodule of R^d. Indeed, if $u, v \in L$ then $\phi(u), \phi(v) \in N$ so $\phi(u+v) = \phi(u) + \phi(v) \in N$ so $u + v \in L$. Similarly, if $u \in L$ and $a \in R$ then $\phi(u) \in N$ so $\phi(au) = a\phi(u) \in N$ so $au \in L$, so L is a submodule as claimed [**1**]. Submodules of R^d are finite free modules, so we can choose a basis $\{p_1, \dots, p_r\}$ for L [**1**]. Put $n_i = \phi(p_i)$ [**1**]; as $p_i \in L$ we have $n_i \in N$ [**1**]. I claim that the elements $n_1, \dots, n_r$ generate N. Indeed, suppose $n \in N$. Then $n \in M$ and the homomorphism $\phi\colon R^d \to M$ is surjective so we have $n = \phi(u)$ for some $u \in R^d$ [**1**]. As $\phi(u) = n \in N$ we see that $u \in L$ [**1**], so u can be written in the form $u = v_1 p_1 + \dots + v_r p_r$ for some $v_1, \dots, v_r \in R$ [**1**]. It follows that

$$n = \phi(u) = v_1 \phi(p_1) + \dots + v_r \phi(p_r) = v_1 n_1 + \dots + v_r n_r.[\mathbf{1}]$$

This shows that the elements $n_1, \dots, n_r$ generate N as claimed, so N is finitely generated. [**1**]

(ii) **[unseen]**

(a) For $v \in M_B$ we have $(x^3 - 27)v = (B^3 - 27\,I)v$, but

$$B^2 = \begin{pmatrix} 0 & 0 & 3 \\ 3 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 3 \\ 3 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 9 & 0 \\ 0 & 0 & 9 \\ 9 & 0 & 0 \end{pmatrix}$$

$$B^3 = \begin{pmatrix} 0 & 0 & 3 \\ 3 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix} \begin{pmatrix} 0 & 9 & 0 \\ 0 & 0 & 9 \\ 9 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 27 & 0 & 0 \\ 0 & 27 & 0 \\ 0 & 0 & 27 \end{pmatrix} = 27\,I,$$

so $(x^3 - 27)v = 0$ as claimed [**2**]. Similarly, we have

$$A^2 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \\ 3 & 3 & 3 \end{pmatrix} = 3A,$$

so for $u \in M_A$ we have $x(x-3)u = (A^2 - 3A)u = 0$ [**1**]. We can now multiply by $(x+3)$ to deduce that $(x^3 - 9x)u = (x+3)x(x-3)u = 0$. [**1**]

(b) Now consider a homomorphism $\gamma\colon M_A \to M_B$, given by $\gamma(u) = Cu$ say. As $\gamma(u) \in M_B$ we have $(x^3 - 27)\gamma(u) = 0$ [**1**]. We can also apply γ to the relation $(x^3 - 9x)u = 0$ to see that $(x^3 - 9x)\gamma(u) = 0$ [**2**]. Subtracting these two equations gives $(9x - 27)\gamma(u) = 0$, and we can divide by 9 to deduce that $(x - 3)\gamma(u) = 0$ [**2**].

(c) Suppose we have $v = (x, y, z) \in \operatorname{im}(\gamma)$. The $v = \gamma(u)$ for some u, so $(x-3)v = (x-3)\gamma(u) = 0$ [**2**]. However, $v \in M_B$ so $xv = Bv$, so

$$(x-3)v = (B - 3I)v = \begin{pmatrix} -3 & 0 & 3 \\ 3 & -3 & 0 \\ 0 & 3 & -3 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 3(z-x) \\ 3(x-y) \\ 3(y-z) \end{pmatrix} [\mathbf{1}].$$

As this is zero, we must have $x = y = z$ and so $v = (x, x, x) \in V$ [**1**].

(4) (i) [**bookwork**]As a and b are coprime, there exist elements $x, y \in R$ such that $xa+yb = 1$ [**1**]. Consider a homomorphism $\alpha\colon M \to N$. For each $m \in M$ we have $am = 0$ and so $a\alpha(m) = \alpha(am) = 0$ [**1**]. On the other hand, we also have $\alpha(m) \in N$ and $bN = \{0\}$ so $b\alpha(m) = 0$ [**2**]. It follows that

$$\alpha(m) = 1.\alpha(m) = (xa + yb)\alpha(m)[\mathbf{1}] = x(a\alpha(m)) + y(b\alpha(m)) = 0 + 0 = 0[\mathbf{1}],$$

so $\alpha = 0$ as required.

(ii) [**unseen**]

(a) Put $a = |L|$ and $b = |M/N|$. By Lagrange's theorem, we have $ax = 0$ for all $x \in L$ and $by = 0$ for all $y \in M/N$. It follows from the above that any homomorphism from L to M/N is zero. [**2**]

(b) Now consider a homomorphism $\alpha\colon L \to M$. By the above, we must have $\pi\alpha = 0\colon L \to M/N$ [**2**]. This means that for all $x \in L$ we have $\pi(\alpha(x)) = \alpha(x) + N = 0 + N$, so $\alpha(x) \in N$. It follows that $\alpha(L) \subseteq N$ as claimed. [**2**]

(iii) (a) [**similar examples seen**]The function $f(t) = t^3 - t$ gives an element of U, but $D.(t^3 - t) = 3t^2 - 1$ takes the value -1 at $t = 0$, so it does not lie in U. Thus, U is not closed under multiplication by D, so it is not an $\mathbb{R}[D]$-submodule. [**3**]

(b) [**This was on a probem sheet**] I claim that W_d is generated by the element t^d. Indeed, we have

$$D^k t^d = d(d-1)\dots(d-k+1)t^{d-k} = \frac{d!}{(d-k)!}t^{d-k}[\mathbf{2}].$$

Thus, for any element $f(t) = \sum_{i=0}^{d} a_i t^i \in W_d$ we can put $p(D) = \sum_i (d!/i!)a_i D^{d-i}$ and we find that $p(D)t^d = f(t)$, so $f(t) \in \mathbb{R}[D].t^d$ as required [**2**].

(c) [**similar examples seen**]For $g(t) = p\sin(t) + q\cos(t) \in V$, we have

$$g'(t) = p\cos(t) - q\cos(t)$$
$$g''(t) = -p\sin(t) - q\cos(t) = -g(t)$$

so $(D^2 + 1)g(t) = 0$ [**2**]. On the other hand, if $f(t) \in W_d$ then the $(d+1)$'st derivative of $f(t)$ is zero, so $D^{d+1}.f(t) = 0$ [**3**]. As D^{d+1} and $D^2 + 1$ are coprime, we deduce that the only homomorphism from W_d to V is zero. [**1**]

(5) (i) **[bookwork]**
Suppose that a and b are coprime. We can then find $x, y \in R$ with $xa + yb = 1$ **[1]**. Given an element $(v + Ra, w + Rb) \in R/a \times R/b$, put $t = ybv + xaw \in R$ **[2]**. We find that

$$t = (1 - xa)v + xaw = v + (xw - xv)a = v \pmod{a} \textbf{[1]}$$
$$t = ybv + (1 - yb)w = w + (yv - yw)b = w \pmod{b} \textbf{[1]}$$

so

$$\phi(t + Rab) = (u + Ra, u + Rb) = (v + Ra, w + Rb).$$

This shows that ϕ is surjective. **[1]**
Now suppose we have an element $u + Rab \in R/ab$ with $\phi(u + Rab) = (u + Ra, u + Rb) = (0 + Ra, 0 + Rb)$. This means that $u \in Ra$ and $u \in Rb$, so $u = pa = qb$ for some $p, q \in R$ **[1]**. It follows that

$$u = (xa + yb)u = xau + ybu = xaqb + ybpa = (xq + yp)ab,$$

so $u \in Rab$ and $u + Rab = 0 + Rab$ **[2]**. This shows that ϕ is injective, and thus an isomorphism **[1]**.

(ii) **[unseen]**Conversely, suppose that ϕ is surjective, so we can find an element $u \in R$ with $\phi(u + Rab) = (1 + Ra, 0 + Rb)$ **[2]**. This means that $u = 1 \pmod{a}$ and $u = 0 \pmod{b}$, so $u = 1 + xa$ and $u = yb$ for some $x, y \in R$ **[2]**. As $1 + xa = yb$ we have $(-x)a + yb = 1$, showing that a and b are coprime **[2]**

(iii) **[bookwork]**We can define a ring homomorphism $\alpha\colon \mathbb{C}[x] \to \mathbb{C}$ by $\alpha(f) = f(\lambda)$ **[1]**. For any $z \in \mathbb{C}$, we can regard z as a constant polynomial and then we have $\alpha(z) = z$; this shows that α is surjective **[1]**. We have $\alpha(f) = 0$ iff $f(\lambda) = 0$ iff $f(x)$ is divisible by $x - \lambda$, so $\ker(\alpha) = \mathbb{C}[x](x - \lambda)$ **[1]**. The first isomorphism theorem for rings thus gives an isomorphism $\overline{\alpha}\colon \mathbb{C}[x]/(x - \lambda) = \mathbb{C}[x]/\ker(al) \to \operatorname{im}(\alpha) = \mathbb{C}$ **[1]**.

(iv) [**The isomorphism** $\mathbb{C}[x]/(x - \lambda)(x - \mu) \simeq \mathbb{C} \times \mathbb{C}$ **will be discussed in lectures**]
Note that if λ and μ are complex numbers with $\lambda \neq \mu$, then $(x - \lambda) - (x - \mu) = \lambda - \mu$ is invertible in $\mathbb{C}[x]$, so $x - \lambda$ and $x - \mu$ are coprime **[1]**. Thus, if we choose any four distinct **[1]**complex numbers $\lambda_1, \ldots, \lambda_4$ and put $f(x) = \prod_i (x - \lambda_i)$ **[1]**then the Chinese Remainder Theorem gives

$$\mathbb{C}[x]/f(x) \simeq \prod_i \mathbb{C}[x]/(x - \lambda_i) \simeq \prod_i \mathbb{C}$$

as required **[2]**.