Rings, Modules and Linear Algebra — Exam solutions

1. (i) (a) The characteristic polynomial is the determinant of the matrix

$$tI - A = \begin{pmatrix} 1+t & -1 & -1 & 1 \\ 0 & 1+t & 0 & -1 \\ 0 & 0 & 1+t & 1 \\ 0 & 0 & 0 & 1+t \end{pmatrix}.$$

As this is an upper-triangular matrix, the determinant is just the product of the diagonal entries, which is $(1+t)^4$.

(b) The minimal polynomial is a divisor of the characteristic polynomial, so it must by $(1+t)^k$ for some integer $k \leq 4$. The matrix $I + A$ is clearly nonzero , but

$$(I+A)^2 = \begin{pmatrix} 0 & 1 & 1 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

It follows that the minimal polynomial of A is $(t+1)^2$.

(c) The first two rows of $I + A$ are clearly linearly independent, but the third row is minus the second, and the last row is zero. Thus, the rank is two.

(ii) (a) The dimension of M_B is $n = k_1 + \ldots + k_r$.

(b) The characteristic polynomial of B is $(t-\lambda)^n$.

(c) The minimal polynomial is $(t-\lambda)^{k_r}$.

(d) The rank of $B - \lambda I$ is $n - r$.

(iii) As -1 is the only root of the characteristic polynomial of A, we see that A is conjugate to a block sum of matrices of the form $J(-1,k)$. In the notation of the previous part, we must have $n = 4$ and $k_r = 2$ and $n - r = 2$. It follows that $r = 2$ and $k_2 = 2$ and $k_1 + 2 = k_1 + k_2 = n = 4$ so $k_1 = 2$. Thus A is conjugate to $J(-1,2) \oplus J(-1,2)$, and M_A is isomorphic to $B(-1,2) \oplus B(-1,2)$.

2. (i)
- Step 1: add x times the middle row to the top row.
- Step 2: multiply bottom two rows by -1.
- Step 3: add x times first column to middle column.
- Step 4: subtract first column from last column.
- Step 5: subtract x^2 times bottom row from top row.
- Step 6: add $x+1$ times middle column to last column.
- Step 7: move top row to the bottom.

$$\begin{pmatrix} x & 0 & -1 \\ -1 & x & -1 \\ 0 & -1 & x+1 \end{pmatrix} \xrightarrow{1} \begin{pmatrix} 0 & x^2 & -1-x \\ -1 & x & -1 \\ 0 & -1 & 1+x \end{pmatrix}$$
$$\xrightarrow{2} \begin{pmatrix} 0 & x^2 & -1-x \\ 1 & -x & 1 \\ 0 & 1 & -1-x \end{pmatrix}$$
$$\xrightarrow{3} \begin{pmatrix} 0 & x^2 & -1-x \\ 1 & 0 & 1 \\ 0 & 1 & -1-x \end{pmatrix}$$
$$\xrightarrow{4} \begin{pmatrix} 0 & x^2 & -1-x \\ 1 & 0 & 0 \\ 0 & 1 & -1-x \end{pmatrix}$$
$$\xrightarrow{5} \begin{pmatrix} 0 & 0 & x^3+x^2-x-1 \\ 1 & 0 & 0 \\ 0 & 1 & -1-x \end{pmatrix}$$
$$\xrightarrow{6} \begin{pmatrix} 0 & 0 & x^3+x^2-x-1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$
$$\xrightarrow{7} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & x^3+x^2-x-1 \end{pmatrix}.$$

This gives us a matrix in normal form.

(ii) It follows that

$$N \simeq \mathbb{C}[x]/(x^3+x^2-x-1).$$

(iii) It follows that $N \simeq M_A$, where A is the companion matrix of f, which is

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

(iv) We have $x^3+x^2-x-1 = (x^2-1)(x+1) = (x-1)(x+1)^2$. As $x-1$ and $x+1$ are coprime , The Chinese Remainder Theorem implies that

$$N \simeq \mathbb{C}[x]/(x^3+x^2-x-1) \simeq \mathbb{C}[x]/(x-1) \oplus \mathbb{C}[x]/(x+1)^2 = B(1,1) \oplus B(-1,2).$$

(v) Let α be a homomorphism from M to N. The module N is annihilated by $f(x) := (x-1)(x+1)^2$, and the module $\mathbb{C}[x]/x^3$ is annihilated by $g(x) := x^3$. If $u \in \mathbb{C}[x]/x^3$ we have $f\alpha(u) = 0$ (because $\alpha(u) \in N$) and also $g\alpha(u) = \alpha(gu) = \alpha(0) = 0$. As f and g are coprime we have $af+bg = 1$ for some $a, b \in \mathbb{C}[x]$ and thus $\alpha(u) = af\alpha(u)+bg\alpha(u) = 0$. Thus $\alpha = 0$.

3. (i) Any Abelian group M of order p^4 can be written as a direct sum of groups of the form $\mathbb{Z}_{p^k}$ with $1 \leq k \leq 4$. If $M \simeq \mathbb{Z}_{p^{k_1}} \oplus \ldots \mathbb{Z}_{p^{k_r}}$ then

$$p^4 = |M| = p^{k_1} \times \ldots \times p^{k_r} = p^{k_1+\ldots+k_r},$$

so $k_1 + \ldots + k_r = 4$. As each k_i is at least 1 this means that $r \leq 4$. Using this and some trial and error we see that the possibilities are as follows:

$$M_1 = \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$$
$$M_2 = \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_{p^2}$$
$$M_3 = \mathbb{Z}_p \oplus \mathbb{Z}_{p^3}$$
$$M_4 = \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$$
$$M_5 = \mathbb{Z}_{p^4}.$$

(ii) We define $F_p^k(M) = \{m \in p^{k-1}M \mid pm = 0\}$. This is a subgroup of M and $pm = 0$ for all $m \in F_p^k(M)$, so it can be regarded as a vector space over the field $\mathbb{Z}/p$. It therefore makes sense to define $f_p^k(M) = \dim_{\mathbb{Z}/p} F_p^k(M)$.

(iii) We have $f_p^1(\mathbb{Z}_{p^k}) = 1$ for all $k > 0$ and $f_p^1(M \oplus N) = f_p^1(M) + f_p^1(N)$, so

$$f_p^1(\mathbb{Z}_{p^{k_1}} \oplus \ldots \mathbb{Z}_{p^{k_r}}) = 1 + \ldots + 1 = r.$$

(iv) The question tells us that $|F_p^1(M)| = p^3$ so $f_p^1(M) = 3$. By (iii), this means that M is a direct sum of three basic modules , and so the only possibility from our list is that $M \simeq M_2$.

(v) Any Abelian group M of order $10000 = 2^4 5^4$ is uniquely the direct sum of an Abelian group P of order 2^4 and an Abelian group Q of order 5^4 . By (i), there are 5 possibilities for P and 5 possibilities for Q , so there are 25 possibilities for the isomorphism type of M.

4. (i) The Chinese Remainder Theorem: Let R be a Euclidean domain, and let a and b be two coprime elements of R. Then R/ab is isomorphic as a ring to $R/a \times R/b$.

Proof. Define $\alpha\colon R \to R/a \times R/b$ by $\alpha(t) = (t + aR, t + bR)$. Note that $\alpha(s + t) = \alpha(s) + \alpha(t)$ and $\alpha(st) = \alpha(s)\alpha(t)$ and $\alpha(1) = 1$, so α is a homomorphism of rings .
As a and b are coprime, we have $xa + yb = 1$ for some $x, y \in R$.
Suppose that $\alpha(t) = (0, 0)$. Then $t + aR$ is the zero coset $0 + aR$, so t is divisible by a, say $t = au$ for some u . Similarly $t = bv$ for some v. This means that

$$t = 1.t = (xa + yb)t = xat + ybt = xa(bv) + yb(au) = (xv + yu)ab,$$

so t is divisible by ab . Conversely, if t is divisible by ab then it is divisible by both a and b, so $\alpha(t) = (0, 0)$. Thus $\ker(\alpha) = Rab$.
Now suppose we have some element $(u + aR, v + bR) \in R/a \times R/b$. Consider the element $t = ybu + xav \in R$. Note that $t = (1 - xa)u + xav = u + xa(v - u) = u \pmod a$ and $t = ybu + (1 - yb)v = v + yb(u - v) = v \pmod b$, so $\alpha(t) = (t + Ra, t + Rb) = (u + Ra, v + Rb)$. This shows that α is surjective. Thus, the First Isomorphism Theorem for rings says that $R/ab \simeq R/a \oplus R/b$. □

(ii) Using the Euclidean algorithm or trial and error we find that $1 = (-2) \times 7 + 3 \times 5$. We thus take $e = 3 \times 5 = 15$, so clearly $e = 0 \pmod 5$ and $e = 2 \times 7 + 1 = 1 \pmod 7$. In $\mathbb{Z}_5$ we have $\overline{e}^2 - \overline{e} = \overline{0}^2 - \overline{0} = \overline{0}$ and in $\mathbb{Z}_7$ we have $\overline{e}^2 - \overline{e} = \overline{1}^2 - \overline{1} = \overline{0}$ so $\overline{e}^2 = \overline{e}$ in $\mathbb{Z}_5 \times \mathbb{Z}_7 \simeq \mathbb{Z}_{35}$.

(iii) For any elements $m \in M$ and $n \in N$ we have $bm = cn = 0$ so $bc(m+n) = c(bm)+b(cn) = 0$; thus $bc(M + N) = 0$. Also, as b and c are both coprime to a, their product bc is also coprime to a , so $xa + ybc = 1$ for some $x, y \in R$. If $u \in L \cap (M + N)$ then $au = 0$ (because $u \in L$) and $bcu = 0$ (because $u \in M + N$) so $u = xau + ybcu = 0$. Thus $L \cap (M + N) = \{0\}$.

5. (i) The First Isomorphism Theorem for rings: Let $\alpha\colon R \to S$ be a ring homomorphism , and let I be the kernel of α . Then there is a ring homomorphism $\overline{\alpha}\colon R/I \to \text{image}(\alpha)$ given by $\overline{\alpha}(a + I) = \alpha(a)$, and moreover this is an isomorphism .

(ii) Define $\alpha\colon \mathbb{R}[x] \to \mathbb{C}$ by $\alpha(f) = f(i)$; this is clearly a ring homomorphism . Any complex number $a+ib$ can be written as $\alpha(a+bx)$, so α is surjective . We have $\alpha(x^2+1) = i^2+1 = 0$, so the ideal generated by $x^2 + 1$ is contained in the kernel of α . Conversely, suppose

that $f \in \ker(\alpha)$. By the division algorithm we can write $f(x) = q(x)(x^2+1) + a + bx$ for some $a, b, \in \mathbb{R}$. We then have $\alpha(f) = f(i) = q(i)(i^2+1) + a + bi = a + bi$. As $\alpha(f) = 0$ we have $a + bi = 0$ so $a = b = 0$, so $f(x) = q(x)(x^2+1)$, so f lies in the ideal generated by $x^2 + 1$. Thus $\ker(\alpha) = \mathbb{R}[x](x^2+1)$, and the First Isomorphism Theorem tells us that $\mathbb{R}[x]/(x^2+1) \simeq \text{image}(\alpha) = \mathbb{C}$.

(iii) (a) It is clear that $\alpha(1) = 1$. Now suppose we have elements $u = a + bi$ and $v = c + di$ in $\mathbb{Z}[i]$. Clearly $\alpha(u + v) = a + c - 2b - 2d = \alpha(u) + \alpha(v)$. Moreover, we have

$$\alpha(u)\alpha(v) = \overline{a - 2bc - 2d} = \overline{ac + 4bd - 2(bc + ad)} = \overline{ac - bd - 2(bc + ad)}$$

(because $4 = -1 \pmod 5$). We also have

$$\alpha(uv) = \alpha((ac - bd) + (ad + bc)i) = \overline{ac - bd - 2(bc + ad)},$$

so $\alpha(uv) = \alpha(u)\alpha(v)$, so α is a ring homomorphism .

Any element $\overline{a} \in \mathbb{Z}_5$ can be written as $\alpha(a + 0i)$, so α is surjective .

(b) We have $\alpha(2 + i) = \overline{2 - 2} = \overline{0}$, so $2 + i \in \ker(\alpha) = \mathbb{Z}[i]q$, so $2 + i$ is divisible by q.

(c) By the above we have $2 + i = qu$ for some $u \in \mathbb{Z}[i]$. As $2 + i$ is irreducible, either q or u must be a unit. If q were a unit we would have $\ker(\alpha) = \mathbb{Z}[i]q = \mathbb{Z}[i]$ so $\alpha = 0$, which is clearly false. Thus u is a unit, so $\ker(\alpha) = \mathbb{Z}[i]q = \mathbb{Z}[i](2 + i)$. The First Isomorphism Theorem now tells us that $\mathbb{Z}[i]/(2+i) = \mathbb{Z}[i]/\ker(\alpha) \simeq \text{image}(\alpha) = \mathbb{Z}_5$.