Homework 9

Jaden Wang

Problem (1)**.** Suppose $N = \langle a_1, \ldots, a_n \rangle$ and $M/N = \langle \overline{b_1}, \ldots, \overline{b_m} \rangle$. Given $x \in M$, then

$$\overline{x} = r_1\overline{b_1} + \cdots r_m\overline{b_m}$$

Then we know that $x - (r_1b_1 + r_mb_m) = y \in N$, *i.e.*

$$x - (r_1b_1 + \cdots + r_mb_m) = s_1a_1 + s_na_n$$
$$x = r_1b_1 + \cdots r_mb_m + s_1a_1 + \cdots s_na_n$$

Hence $x \in \langle a_1, \ldots, a_n, b_1, b_m \rangle$ and thus $M = \langle a_1, \ldots, a_n, b_1, b_m \rangle$ is finitely generated.

Problem (2)**.**

(a) Since $A = \{x_1, \ldots, x_n\}$ is a maximal set of linearly independent elements contained in N, we see that N is rank at least n. But since A generates N, the rank of N is at most n so it equals n. It suffices to show that N satisfies the universal property of free modules. There is a canonical injection set map $\iota : A \to N$. Since elements of A are linearly independent, there is no relation among the elements (otherwise the relations would yield a dependence). Since elements of A generate N, given any module L, we can construct a module homomorphism $\Phi : N \to L$ by simply specifying a set map $\phi : A \to L$. Any such set map would do due to the lack of relations and yield a unique homomorphism Φ. Thus we have the commutative diagram

$$\begin{array}{ccc} A & \xhookrightarrow{\iota} & N \\ & \searrow^{\phi} & \downarrow{\scriptstyle \exists! \Phi} \\ & & L \end{array}$$

Therefore, N is free.

If $M = N$ then $M/N = 0$ is clearly torsion. Suppose there exists $x \in M - N$, then $A \cup \{x\}$ must be a linearly dependent set as A is maximal, so $x = r_1x_1 + \cdots + r_nx_n \in N$ where r_i is not all zero. Take r to be the product of nonzero coefficients so $r \neq 0$ as R is an integral domain, then clearly $rx = 0$ and $r.(x + N) = rx + N = 0 + N = N$ so M/N is torsion.

(b) Since M contains a module of rank n, M has rank at least n. Since M/N is torsion, given any $x \in M$, we see that there exists $r \neq 0$ s.t. $rx \in N$, *i.e.*

$$rx = r_1 x_1 + \cdots + r_n x_n$$

Therefore, $A \cup \{x\}$ is always linearly dependent, so the rank of A is at most n and therefore equals n.

Problem (3)**.** The rank of M is at least 1 since it contains $\langle 2 \rangle$. But since $x2 - 2x = 0$ is a linear dependence relation between the generators, we conclude that the rank is less than 2 and therefore equals 1.

Problem (4)**.** Given two 3×3 matrices A and B.

($\Rightarrow$) : Suppose $A \sim B$, then they must have the same rational canonical form, which completes describe all invariant factors including the minimal polynomial, and therefore characteristic polynomial as the product of all invariant factors.

($\Leftarrow$) : Suppose A and B have the same characteristic polynomial $c(x) = (x - a)($ and $m(x) = ()$. Consider the partition of 3: 3, $2 + 1$, and $1 + 1 + 1$. If the degree of $m(x)$ is 3, then the rational canonical form of both A and B is just the companion matrix of $m(x)$ and therefore the same. In the second partition, *i.e.* $\deg m(x) = 2$ (by divisibility condition), then there can only be one other invariant factor which has degree 1 and is completely determined by $c(x)/m(x)$. Thus they have the same RCF. In the third partition, since $\deg m(x) = 1$, the other invariant factors must be two $m(x)$ as well so they again have the same RCF. Thus in all cases $A \sim B$.

Consider

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

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

We see that $m_A(x) = m_B(x) = (x-1)^2$ and $c_A(x) = c_B(x) = (x-1)^4$, but their RCFs are just themselves and clearly do not equal so $A \not\sim B$.

Problem (5)**.**

Case (1)*.* F is not of characteristic 2 and $i \notin F$.

Since $F[x]$ is a UFD, $x+1$ and $x-1$ are irreducibles and therefore primes. And since $x+1, x-1$ doesn't divide x^2+1, we have that $x+1, x-1, x^2+1$ are pairwise comaximal.

Next, we know that $c(x) = (x+1)^5(x-1)^3(x^2+1)^3$ and $(x+1)(x-1)(x^2+1)|m(x)$. Moreover, since we cannot further decompose prime-powers, we know $(x+1)^2$ and $(x^2+1)^2$ also divide $m(x)$. Hence $(x+1)^2(x-1)(x^2+1)^2|m(x)$. No other terms are comaximal with $(x+1)^2(x-1)(x^2+1)^2$ so it is the largest invariant factor we can get: $m(x) = (x+1)^2(x-1)(x^2+1)^2$. Next we split $(x^2+1)(x+1)(x-1)$ into $(x+1)(x-1)$ and (x^2+1) and recombine the latter with $(x+1)^2(x-1)$. Thus, by the Chinese Remainder Theorem,

$$V \cong F[x]/\langle (x+1)(x-1)\rangle \oplus F[x]/\langle (x^2+1)(x+1)^2(x-1)\rangle \oplus F[x]/\langle (x^2+1)^2(x+1)^2(x-1)\rangle$$

which satisfies the divisibility criterion. By uniqueness we obtain the invariant factors.

The elementary divisors follow: $x+1, x-1, x^2+1, (x+1)^2, x-1, (x^2+1)^2, (x+1)^2, x-1$.

Case (2)*.* F is characteristic 2. Then the annihilators are $(x+1)^2$, FIX $(x+1)(x^2+1)^2 = (x+1)^5$, $(x^2+1)(x+1)^2 = (x+1)^4$, and $(x+1)^3$. The minimal polynomial is $m(x) = (x+1)^5$, and we have $(x+1)^2|(x+1)^3|(x+1)^4|m(x)$ as invariant factors. The elementary divisors are $(x+1)^2, (x+1)^3, (x+1)^4, (x+1)^5$.

Case (3)*.* $F = F(i)$. Then the annihilators are $(x+1)^2$, $(x-1)(x+1)(x+i)^2(x-i)^2$, $(x+i)(x-i)(x+1)(x-1)$, and $(x+1)^2(x-1)$. We have $x+1|(x+1)(x-1)(x+i)(x-i)|(x+1)^2(x-1)(x+i)^2(x-i)^2$ as invariant factors, and elementary divisors are $x+1, x+1, x-1, x+i, x-i, (x+1)^2, (x-1), (x+i)^2, (x-i)^2$.

Problem (6)**.** Note: most computations were done on scratch papers.

$$xI - A = \begin{pmatrix} x & -1 & -1 & -1 \\ -1 & x & -1 & -1 \\ -1 & -1 & x & -1 \\ -1 & -1 & -1 & x \end{pmatrix}$$

Using the notation of Exercise 35 of 12.3, we see that $d_0 = 1$, $d_1 = \gcd(x, -1) = 1$, $d_2 = \gcd(x^2 - 1, x + 1) = x + 1$, $d_3 = \gcd((x-2)(x+1)^2, -(x+1)^2) = (x+1)^2$, and $d_4 = (x-3)(x+1)^3$. Hence the Smith Normal Form S has diagonal entries $S_{11} = d_1/d_0 = 1$, $S_{22} = d_2/d_1 = x + 1$, $S_{33} = d_3/d_2 = x + 1$, and $S_{44} = d_4/d_3 = (x-3)(x+1) = x^2 - 2x - 3$, which are the invariant factors of A. It follows that the RCF of A is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 1 & 2 \end{pmatrix}$$

The elementary divisors are $x + 1, x + 1, x + 1, x - 3$, all linear factors over $\mathbb{Q}$. Hence the JCF of A is simply the diagonal matrix of eigenvalues:

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

Problem (7)**.**

(a) For $k \leq n$, $p^k | a$ so $\langle a \rangle \leq \langle p^k \rangle$. Thus by the third isomorphism theorem,

$$\begin{aligned} \frac{p^{k-1}M}{p^k M} &= \frac{p^{k-1}R/\langle a \rangle}{p^k R/\langle a \rangle} \\ &= \frac{p^{k-1}\langle 1 \rangle/\langle a \rangle}{p^k \langle 1 \rangle/\langle a \rangle} \\ &= \frac{\langle p^{k-1} \rangle}{\langle p^k \rangle} \end{aligned}$$

Moreover, it is easy to see that $\phi : \langle p^{k-1} \rangle \to R/\langle p \rangle, p^{k-1} \mapsto 1 + \langle p \rangle$ is a surjective module homomorphism: the additive order of 1 is p, which divides the additive order of p^{k-1} which is $\frac{a}{p^{k-1}}$, a p-power, so ϕ is well-defined. Then $\ker \phi = \langle p^k \rangle$ so by the first isomorphism theorem,

$$\frac{p^{k-1}M}{p^k M} \cong \frac{\langle p^{k-1} \rangle}{\langle p^k \rangle} \cong \frac{R}{\langle p \rangle}.$$

When $k > n$, we have $k - 1 \geq n$ so $\langle p^k \rangle \leq \langle p^{k-1} \rangle \leq \langle a \rangle$. Since $M = R/\langle a \rangle$ is generated by $1 + \langle a \rangle$, and $p^{k-1} + \langle a \rangle = p^k + \langle a \rangle = \langle a \rangle$. That is, multiplication by p^{k-1} or p^k is the trivial map. Thus $p^{k-1}M = p^k M$ is trivial so the quotient is trivial.

(b) First we prove a claim.

Claim 0.1. If M is a finitely generated torsion R-module, then $p^{k-1}M/p^kM \cong F^{n_k}$, where $F = R/\langle p\rangle$ and n_k is the number of elementary divisors p^ℓ of M for any $\ell \geq k$.

Proof. By the structure theorem, since M is torsion we have $M \cong R/\langle a_1\rangle \oplus \cdots \oplus R/\langle a_n\rangle$. Then

$$p^{k-1}M/p^kM \cong \frac{p^{k-1}R/\langle a_1\rangle}{p^kR/\langle a_1\rangle} \oplus \cdots \oplus \frac{p^{k-1}R/\langle a_n\rangle}{p^kR/\langle a_n\rangle}.$$

By part a), if $p^k | a_i$, *i.e.* a_i has elementary divisor p^ℓ with $\ell \geq k$, then we get a copy of F in the ith component. Otherwise we get a 0. The claim easily follows. □

Now suppose $M_1 \cong M_2$ as finitely generated torsion R-modules and $k \geq 0$, then they are isomorphic to the same direct sums of cyclic modules. By the claim, we show the first part of the problem. Next, we can obtain the exact number of p^k in M by $n_k - n_{k+1}$. Since p and k are arbitrary, we show that M_1 and M_2 must have the same number of any p^k and therefore the same set of elementary divisors.