MAT 612 **Exam 1 (take-home)** Name SOLUTIONS
2/22/2010 (due Monday 3/1/2010, 5 pm)
90 points

All rings are commutative with 1. All modules are unital.

1.(20) (a) Suppose $M$ and $N$ are free $R$-modules of finite rank. Prove that $\operatorname{Hom}_R(M, N)$ is a free $R$-module, and determine its rank.

Hint: Use the case where $R$ is a field for guidance.

(b) Prove, if $N$ is a free $R$-module, then $\operatorname{Hom}_R(M, N)$ is isomorphic to $\operatorname{Hom}_R(M/\operatorname{Tor}(M), N)$ for any $R$-module $M$.

2.(25) (a) Let $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ be an exact sequence of $R$-modules. Suppose there is an $R$-module homomorphism $\sigma\colon P \longrightarrow N$ satisfying $g \circ \sigma = \mathrm{id}_P$. Prove there is an $R$-module homomorphism $\pi\colon N \longrightarrow M$ satisfying $\pi \circ f = \mathrm{id}_M$.

Hint: One may assume without loss that $M$ is a submodule of $N$ and $f$ is the inclusion map.

(b) Under the same hypotheses as in part (a), prove that $N$ is isomorphic to $M \oplus P$.

Hint: Use $\sigma$ and $\pi$ to define a homomorphism from $N$ to $M \oplus P$, and then apply the (short) five lemma.

(c) Prove, if $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ is exact, and $P$ is a free module, then $N \cong M \oplus P$.

(d) Suppose $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ is exact, and suppose there is an $R$-module $Q$ such that $P \oplus Q$ is a free module. Prove that $N \cong M \oplus P$.

(e) Suppose $P$ has the property that, for any module $N$ and any surjective homomorphism $g\colon N \longrightarrow P$, there is a homomorphism $\sigma\colon P \longrightarrow N$ such that $g \circ \sigma = \mathrm{id}_P$. Prove that there is a module $Q$ such that $P \oplus Q$ is a free module.

(f) An $R$-module $P$ is said to be *projective* if it satisfies the hypothesis of part (e). Prove, if $R$ is a PID and $P$ is an $R$-module, then $P$ is projective if and only if $P$ is free.

3.(10) Prove: If $R$ is a PID, then an ideal $I$ is primary if and only if $I$ is irreducible.

4.(15) (a) Find a presentation and free resolution of the $\mathbb{Z}$-module $\mathbb{Z}_2 \oplus \mathbb{Z}_{30} \oplus \mathbb{Z}$.

(b) Let $M$ be the $\mathbb{Z}$-module generated by three elements $v_1, v_2, v_3$ subject to the relations

$$\begin{aligned} 2v_1 - 4v_2 - 2v_3 &= 0 \\ 10v_1 - 6v_2 + 4v_3 &= 0 \\ 6v_1 - 12v_2 - 6v_3 &= 0. \end{aligned}$$

Find a free resolution of $M$ and the invariant factor decomposition of $M$, and determine $\operatorname{rank}(M)$ and $\operatorname{Tor}(M)$.

5.(5) Let $M$ be the $\mathbb{Z}$-module of Problem 4(b). For each prime ideal $P$ of $\mathbb{Z}$, find the set $M_P = \{x \in M \mid \sqrt{\operatorname{ann}(x)} = P\}$, and show that $M = \bigoplus_P M_P$.

6.(15) Suppose $\mathbb{k}$ is an algebraically closed field, and $R = \mathbb{k}[x]$. Since $\mathbb{k}$ is algebraically closed, the irreducible elements of $R$ are of the form $x - a$, for $a \in \mathbb{k}$, up to multiplication by units. Suppose $M$ is a cyclic $R$-module, whose annihilator is a nonzero primary ideal of $R$. Show that $M$ has a (free) $\mathbb{k}$-basis $\mathcal{B}$ such that the matrix of the linear transformation $T\colon M \longrightarrow M$ given by $T(v) = x \cdot v$ relative to $\mathcal{B}$ has the form

$$\begin{bmatrix} a & 1 & 0 & \cdots & 0 \\ 0 & a & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & & 0 \\ \vdots & \vdots & & \ddots & 1 \\ 0 & 0 & \cdots & \cdots & a \end{bmatrix}.$$

① (a) We may assume $M \cong R^n$ and $N \cong R^m$ for non-negative integers $m$ and $n$. Then a module homomorphism $f: R^n \longrightarrow R^m$ is given by $f((r_1, \dots, r_n)) = (f_1(r_1, \dots, r_n), \dots, f_m(r_1, \dots, r_n))$ where $f_i: R^n \to R$ is a homomorphism. This yields an isomorphism $\mathrm{Hom}_R(R^n, R^m) \longrightarrow \underbrace{\mathrm{Hom}_R(R^n, R) \times \cdots \times \mathrm{Hom}_R(R^n, R)}_{m \text{ factors}}$

By exercise 12.1.__, $\mathrm{Hom}_R(R^n, R)$ is isomorphic to $R^n$, hence $\mathrm{Hom}_R(R^n, R^m)$ is isomorphic to $(R^n)^m$, or $R^{nm}$, a free module. Alternate proof: Let $\{e_1, \dots, e_n\}$ be a free basis for $M$, and $\{f_1, \dots, f_m\}$ a free basis for $N$. Define $\varphi_{ij} \in \mathrm{Hom}_R(R^n, R^m)$ by $\varphi_{ij}(e_j) = f_i$; $\varphi_{ij}$ extends to a unique homomorphism by freeness. Claim $\{\varphi_{ij} \mid 1 \le i \le m, 1 \le j \le n\}$ is a free basis of $\mathrm{Hom}_R(M, N)$. Indeed, if $\varphi \in \mathrm{Hom}_R(M, N)$ let $r_{ij} \in R$ with $\varphi(e_j) = \sum_{i=1}^{m} r_{ij} f_i$ for $1 \le j \le n$. Then $\varphi = \sum_{i,j} r_{ij} \varphi_{ij}$; indeed, $\varphi(e_j) = \sum_i r_{ij} f_i = \sum_i r_{ij} \varphi_{ij}(e_j)$, and since the $e_j$ generate $M$, this implies the functions are equal. For the same reason, if $\sum_{i,j} r_{ij} \varphi_{ij} = 0_{\mathrm{Hom}_R(M,N)}$, then $r_{ij} = 0 \; \forall \, i, j$. Thus $\{\varphi_{ij}\}$ is a linearly independent generating set, hence $\mathrm{Hom}_R(M, N)$ is a free $R$-module (whose rank is $\mathrm{rank}(M) \cdot \mathrm{rank}(N)$. □

① (b) Let $f \in \mathrm{Hom}_R(M, N)$. If $x \in \mathrm{Tor}(M)$, then $\exists\, r \in R \setminus \{0_R\}$ with $rx = 0_M$. Then $rf(x) = f(rx) = f(0_M) = 0_N$. Since $N$ is free, it is torsionfree, so $f(x) = 0$. Let $\overline{f} : M/\mathrm{Tor}(M) \longrightarrow N$ be defined by $\overline{f}(x + \mathrm{Tor}(M)) = f(x)$. Since $f(\mathrm{Tor}(M)) = 0$, $\overline{f}$ is well-defined. ( $x - y \in \mathrm{Tor}(M) \Longrightarrow f(x) - f(y) = f(x-y) = 0 \Longrightarrow f(x) = f(y)$ ). Clearly the map $\Phi : \mathrm{Hom}_R(M, N) \longrightarrow \mathrm{Hom}_R(M/\mathrm{Tor}(M), N)$ given by $\Phi(f) = \overline{f}$ is a homomorphism. If $\overline{f} = 0$ then $f = 0$, so $\Phi$ is injective, and if $g : M/\mathrm{Tor}(M) \longrightarrow N$, then $g = \overline{f}$ where $f : M \longrightarrow N$ is given by $f = g \circ q$ where $q$ is the canonical quotient map. So $\Phi$ is surjective. Thus $\mathrm{Hom}_R(M, N)$ is isomorphic to $\mathrm{Hom}_R(M/\mathrm{Tor}(M), N)$. □

② (a) Let $n \in N$. Then $g(n - \sigma(g(n))) = g(n) - (g \circ \sigma)(g(n)) = g(n) - g(n) = 0_P$, hence $n - \sigma(g(n)) \in \ker(g)$, so $n - \sigma(g(n)) \in \mathrm{im}(f)$ by exactness. Since $f$ is injective, there is a unique $m \in M$ such that $f(m) = n - \sigma(g(n))$. We define $\pi : N \longrightarrow M$ by $\pi(n) = m$, for $f(m) = n - \sigma g(n)$. If $f(m_1) = n_1 - (\sigma \circ g)(n_1)$ and $f(m_2) = n_2 - (\sigma \circ g)(n_2)$, then $f(m_1 + m_2) = f(m_1) + f(m_2) = n_1 + n_2 - (\sigma \circ g)(n_1) - \sigma \circ g(n_2)$ $= (n_1 + n_2) - (\sigma \circ g)(n_1 + n_2)$, so $\pi(n_1 + n_2) = m_1 + m_2 = \pi(n_1) + \pi(n_2)$. Similarly, $\pi(rn) = r\pi(n)$. Thus $\pi$ is a homomorphism. By definition, $\pi(f(m)) = m$ for all $m \in M$, so $\pi \circ f = \mathrm{id}_N$.

(b) Let $\beta : N \longrightarrow M \;\; P$ be given by $\beta(m) = (\pi(m), g(m))$. Then the following diagram commutes:

$$\begin{tikzcd}
1 \arrow[r] & M \arrow[r, "f"] \arrow[d, "\mathrm{id}_M"] & N \arrow[r, "g"] \arrow[d, "\beta"] & P \arrow[r] \arrow[d, "\mathrm{id}_P"] & 0 \\
1 \arrow[r] & M \arrow[r] & M \oplus P \arrow[r] & P \arrow[r] & 0
\end{tikzcd}$$

$m \longmapsto (m, 0)$

$(m, p) \longmapsto p$

Then $\beta$ is an isomorphism by the five lemma.

(c) Let $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ with $P$ free.
Let $\mathcal{B}$ be a free basis for $P$, and for each $b \in \mathcal{B}$, let $\sigma(b) \in N$ with $g(\sigma(b)) = b$; $\sigma(b)$ exists because $g$ is onto. By freeness, $\sigma$ extends to a homomorphism $\sigma : P \to M$, and $g \circ \sigma = id_P$ because $(g \circ \sigma)(b) = b$ for all $b \in \mathcal{B}$, and $\mathcal{B}$ generates $P$. Then $N \cong M \oplus P$ by (b).

(d) Let $\{(p_\alpha, q_\alpha) \mid \alpha \in \Lambda\}$ be a free basis for $P \oplus Q$.
Define $\hat{\sigma}((p_\alpha, q_\alpha)) = m$ where $g(m) = p_\alpha$; such an $m$ exists because $g$ is onto. By freeness, $\hat{\sigma}$ extends to a (unique) homomorphism $\hat{\sigma} : P \oplus Q \to M$. Define $\sigma : P \to N$ by $\sigma(p) = \hat{\sigma}((p, 0))$. For any $(p, q) \in P \oplus Q$, $g(\hat{\sigma}(p, q)) = p$, since that equation holds for each $(p_\alpha, q_\alpha)$, which generate $P \oplus Q$. Then $g(\sigma(p)) = g(\hat{\sigma}(p, 0)) = p$, hence $g \circ \sigma = id_P$, and then $N \cong M \oplus P$ by (b).

(e) Let $\mathcal{B}$ be a generating set for $P$, and let $F$ be a free module with basis $\mathcal{B}$. ($F = \{v : \mathcal{B} \to R \mid v(x) = 0$ for all but finitely many $x \in \mathcal{B}\}$.) Then there is a surjective homomorphism $g : F \to P$. Let $Q = \ker(g)$. Then we have a short exact sequence $0 \to Q \hookrightarrow F \xrightarrow{g} P \to 0$. By hypothesis the sequence splits, i.e., $\exists\, \sigma : P \to F$ such that $g \circ \sigma = id_P$. Then $F \cong P \oplus Q$ by (b).

(f) By (e), $P$ is isomorphic to a submodule of a free module. Since $R$ is a PID, any submodule of a free $R$-module is free. Thus $P$ is free.

(3) It was shown in class that every irreducible ideal is primary, if $R$ is noetherian, and PID's are noetherian. So we need only prove the converse. Suppose $I$ is a primary ideal

in the PID $R$. Then $I = (p^a)$. Suppose $I = J_1 \cap J_2$ for ideals $J_1, J_2$. Since $R$ is a PID, $J_1 = (m)$ and $J_2 = (n)$ for some $m, n \in R$. Since $I \subseteq J_1$ and $I \subseteq J_2$, both $m$ and $n$ divide $p^a$. Since $R$ is a PID, $R$ is a UFD, and $m$ and $n$ have prime factorizations; since $m \mid p^a$ and $n \mid p^a$, we must have $m = p^k$ and $n = p^l$ for some $k$ and $l$. Then $J_1 \cap J_2 = (p^k) \cap (p^l) = (p^m)$ where $m = \min(k, l)$. Then $(p^a) = I = J_1 \cap J_2 = (p^m)$, so $a = m$, and thus $I = J_1$ or $I = J_2$. Hence $I$ is irreducible.

$M = \mathbb{Z}_2 \oplus \mathbb{Z}_{30} \oplus \mathbb{Z}$

(4) (a) $M$ is generated by $x = (1,0,0)$, $y = (0,1,0)$, and $z = (0,0,1)$, subject to the relations $2x = 0$, $30y = 0$. Then we have a presentation of $M$:

$$\mathbb{Z}^2 \xrightarrow{g} \mathbb{Z}^3 \xrightarrow{f} M \longrightarrow 0$$

Where $f(1,0,0) = x$, $f(0,1,0) = y$, $f(0,0,1) = z$, $g(1,0) = (2,0,0)$, $g(0,1) = (0,30,0)$. (So $g$ has matrix $\begin{bmatrix} 2 & 0 & 0 \\ 0 & 30 & 0 \end{bmatrix}$. In fact $g$ is injective, since $\{(2,0,0), (0,30,0)\}$ is linearly independent in $\mathbb{Z}^3$.

So we have a free resolution of $M$:

$$0 \longrightarrow \mathbb{Z}^2 \xrightarrow{g} \mathbb{Z}^3 \xrightarrow{f} M \longrightarrow 0.$$

(b) By definition, $M$ has presentation

$$\mathbb{Z}^3 \xrightarrow{g} \mathbb{Z}^3 \xrightarrow{f} M \longrightarrow 0$$

where $f(1,0,0) = x$, $f(0,1,0) = y$, $f(0,0,1) = z$, and $g(1,0,0) = (2,-4,-2)$, $g(0,1,0) = (10,-6,4)$, and $g(0,0,1) = (6,-12,-6)$. In other words, $M$ has presentation matrix $\begin{bmatrix} 2 & -4 & -2 \\ 10 & -6 & 4 \\ 6 & -12 & -6 \end{bmatrix}$. Since $\mathbb{Z}$ is a PID,

over

the image of $g$ is a free submodule. The Smith Normal form of $\begin{bmatrix} 2 & -4 & -2 \\ 10 & -6 & 4 \\ 6 & -12 & -6 \end{bmatrix}$ is $\begin{bmatrix} 2 & 0 & 0 \\ 0 & 14 & 0 \\ 0 & 0 & 0 \end{bmatrix}$. Then there is a free basis $\{w_1, w_2, w_3\}$ of $R^3$ so that $\mathrm{im}(g)$ is generated by $\{2w_1, 14w_2\}$. Then a free resolution of $M$ is given by $0 \longrightarrow \mathbb{Z}^2 \xrightarrow{g'} \mathbb{Z}^3 \xrightarrow{f'} M \longrightarrow 0$ where $g'$ has matrix $\begin{bmatrix} 2 & 0 & 0 \\ 0 & 14 & 0 \end{bmatrix}$. To find $f'$ we need to know $w_1, w_2$, and $w_3$. Tracing the row operations that carry $g$ to $g'$, one sees that $(2,-4,-2)$ and $(0,14,14)$ lie in $\mathrm{im}(g)$, and generate $\mathrm{im}(g)$, so we can take $w_1 = (1,-2,-1)$ and $w_2 = (0,1,1)$, and $w_3 = (0,0,1)$ will complete a basis for $R^3$. Then $f'(1,0,0) = v_1 - 2v_2 - v_3$, $f'(0,1,0) = v_2 + v_3$, and $f'(0,0,1) = v_3$.
The invariant factor decomposition of $M$ is $M \cong \mathbb{Z}/2 \oplus \mathbb{Z}/14 \oplus \mathbb{Z}$, $\mathrm{Tor}(M) \cong R/2R \oplus R/14R$ and is generated by $\{v_1 - 2v_2 - v_3, v_2 + v_3\}$, and $\mathrm{rank}(M) = 1$.

(5) Clearly the nonzero primes that annihilate nonzero elements of $M$ are $P = (2)$ and $P = (14)$. For $P = (2)$, $M_P$ is generated by $\{w_1, 7w_2\}$ while for $(P) = (7)$, $M_P$ is generated by $\{2w_2\}$. Since $\mathbb{Z}$ is a domain, $P = 0$ is prime, and $M_P \cong \mathbb{Z}w_3$. Since $\mathbb{Z}/14\mathbb{Z} \cong 7\mathbb{Z}/14\mathbb{Z} \oplus 2\mathbb{Z}/14\mathbb{Z}$ $\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}$, we have $M \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z} \oplus \mathbb{Z}$ $\cong (\mathbb{Z}/2\mathbb{Z} \oplus 7\mathbb{Z}/14\mathbb{Z}) \oplus 2\mathbb{Z}/14\mathbb{Z} \oplus \mathbb{Z} = M_{(2)} \oplus M_{(7)} \oplus M_0$ $= \bigoplus_P M_P$.

(6) By assumption, $M = Rv$ for some $v$, and $\mathrm{ann}(v) = I$ is a nonzero primary ideal of $M$. Since $R = \Bbbk[x]$ is a PID, the primes of $R$ are the irreducibles, which have the form $(x-a)$, $a \in \Bbbk$, since $\Bbbk$ is algebraically closed.

Also, since $R$ is a PID, the primary ideals are generated by powers of primes. Thus $\mathrm{ann}(v) = ((x-a)^n)$ for some $a \in \mathbb{k}$, $n \geq 1$. So let $v_1 = v$, $v_2 = (x-a)\cdot v_1$, $v_3 = (x-a)\cdot v_2$, $\ldots$, $v_{n-1} = (x-a)\cdot v_{n-2}$. Then $(x-a)\cdot v_{n-1} = (x-a)^n v = 0$, so $x \cdot v_{n-1} = a v_{n-1}$. Also, $x \cdot v_{n-2} = a v_{n-2} + v_{n-1}$, $x \cdot v_{n-3} = a v_{n-3} + v_{n-2}$, and so on, ending with $x \cdot v_1 = a v_1 + v_2$.

We claim $\{v_{n-1}, v_{n-2}, \ldots, v_2, v_1\}$ is a $\mathbb{k}$-basis for $V$.

Given the claim, the matrix of $T : V \longrightarrow V$; $T(v) = x \cdot v$, relative to the (ordered) basis $\{v_{n-1}, \ldots, v_1\}$ is

$$\begin{array}{c|c} & \begin{array}{cccccc} v_{n-1} & & & & & v_1 \end{array} \\ \begin{array}{c} v_{n-1} \\ \\ \\ \\ \\ v_1 \end{array} & \begin{bmatrix} a & 1 & 0 & \cdots & & 0 \\ 0 & a & 1 & & & \vdots \\ 0 & 0 & a & & & \\ \vdots & \vdots & \vdots & & & \\ \vdots & \vdots & \vdots & & & \vdots \\ 0 & 0 & 0 & \cdots & 0 & a \end{bmatrix} \end{array}$$

. To prove the claim, observe that

(1) $\{x^k \cdot v \mid k \geq 0\} \subseteq \mathbb{k}v_1 + \cdots + \mathbb{k}v_{n-1}$, and since $v$ generates $V$ (over $R$), $\{x^k \cdot v \mid k \geq 0\}$ spans $V$ (over $\mathbb{k}$), so $\{v_1, \ldots, v_{n-1}\}$ spans $V$ over $\mathbb{k}$, and

(2) If $\sum_{k=1}^{n-1} c_k v_k = 0$, then $\left(\sum_{k=0}^{n-1} c_k (x-a)^k\right) \cdot v = 0$, so $\sum_{k=0}^{n-1} c_k (x-a)^k \in \mathrm{ann}(v)$, contradicting the fact that $\mathrm{ann}(v)$ is generated by $(x-a)^n$ (a polynomial of degree $n$.).