Modern Algebra 2 (MATH 6140)
Test #2
Solution Key

This exam is due Friday, March 21. You are expected to complete three problems, one from each group. Clearly mark which problems are to be graded.

You may use your book, but you may not communicate with others concerning the exam. In order to receive full credit your answer must be **complete**, **legible** and **correct**.

I have neither given nor received aid on this exam.

Name:______________________________

Group 1.

1. Let R be an integral domain. Suppose that every finitely generated R-module is isomorphic to one of the form $R/(a_1) \oplus \cdots \oplus R/(a_k) \oplus (\oplus^r R)$. Show that R is a PID.

Solution. Let $I \lhd R$ be a nonzero ideal. R/I is a cyclic torsion module, so

$$R/I \cong R/(a_1) \oplus \cdots \oplus R/(a_k). \tag{1}$$

Isomorphic modules have the same annihilator, so

$$I = \mathrm{Ann}_R(R/I) = \mathrm{Ann}_R(R/(a_1) \oplus \cdots \oplus R/(a_k)) = (a_1) \cap \cdots \cap (a_k).$$

To show that I is principal, it is enough to show that $\bigcap (a_i)$ is principal.

Claim 1. If ideals J and K are comaximal ($J + K = R$), then $J \cap K = JK$. (Hence if principal ideals (a) and (b) are comaximal, then $(a) \cap (b) = (ab)$ is principal.)

Since J and K are ideals, $JK \subseteq J$ and $JK \subseteq K$, so $JK \subseteq J \cap K$. Moreover, both J and K multiply the larger ideal into the smaller (i.e., $\underline{J}(\underline{J \cap K}) \subseteq \underline{J}\,\underline{K}$ and $(\underline{J \cap K})\underline{K} \subseteq \underline{J}\,\underline{K}$). This yields the reverse inclusion

$$J \cap K = R(J \cap K) = (J + K)(J \cap K) = J(J \cap K) + K(J \cap K) \subseteq JK.$$

Claim 2. $(a_1) \cap \cdots \cap (a_i) = (a_1 a_2 \cdots a_i)$ is comaximal with (a_{i+1}) for all i.

By (1), $R/(a_1) \oplus \cdots \oplus R/(a_k)$ is a cyclic module, so the quotient $R/(a_1) \oplus R/(a_2)$ is cyclic. If (a_1) and (a_2) are not comaximal, then there is a maximal ideal $M \lhd R$ such that $(a_1) + (a_2) \subseteq M$. Tensoring the cyclic R-module $R/(a_1) \oplus R/(a_2)$ with the $(R/M, R)$-bimodule R/M, which is a field, we get a cyclic R/M-vector space

$$R/M \otimes_R (R/(a_1) \oplus R/(a_2)) \cong R/M \oplus R/M.$$

But a cyclic R/M-space is 1-dimensional, and $R/M \oplus R/M$ is 2-dimensional.

Since $C = R/(a_1) \oplus R/(a_2)$ is a cyclic module, it is isomorphic to $R/\mathrm{Ann}_R(C) = R/((a_1) \cap (a_2))$. But (a_1) and (a_2) are comaximal, so $(a_1) \cap (a_2) = (a_1 a_2)$, yielding

$$(R/(a_1) \oplus R/(a_2)) \oplus R/(a_3) \oplus \cdots \oplus R/(a_k) \cong R/(a_1 a_2) \oplus R/(a_3) \oplus \cdots \oplus R/(a_k).$$

This module is still cyclic, so we can repeat the argument.

Altogether, $I = \bigcap (a_i) = (a_1 \cdots a_k)$.

2. Prove or disprove: the rational canonical form of a permutation matrix is a permutation matrix.

Solution. (Discussion) The statement is true for cyclic permutations, and some others, but not for all permutations.

An $n \times n$ permutation matrix is the matrix of a transformation Σ, derived from a permutation $\sigma \in S_n$, that is defined to act on the basis $\mathcal{B} = (e_1, \ldots, e_n)$ by $\Sigma(e_i) = e_{\sigma(i)}$. If $\sigma = (1\ 2\ \cdots\ n)$, then

$$
{}_{\mathcal{B}}[\Sigma]_{\mathcal{B}} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & & 0 & 0 \\ 0 & 1 & 0 & & 0 & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix},
$$

which is the companion matrix for the polynomial $x^n - 1$. Hence $x^n - 1$ is both the characteristic and minimal polynomial for ${}_{\mathcal{B}}[\Sigma]_{\mathcal{B}}$, and ${}_{\mathcal{B}}[\Sigma]_{\mathcal{B}} = \mathrm{RCF}(\Sigma)$.

But now consider a permutation $\tau = \sigma_1 \cdots \sigma_k$ that is a product of k disjoint cyclies of lengths $\ell_1, \ldots, \ell_k$. If T acts on basis elements by $T(e_i) = e_{\tau(i)}$, then $[T]$ is a block diagonal matrix with companion matrices for $x^{\ell_1} - 1, \ldots, x^{\ell_k} - 1$ on the diagonal. Hence the characteristic polynomial for $[T]$ is $\chi_T(x) = \prod(x^{\ell_i} - 1)$ and the minimal polynomial is $m_T(x) = \mathrm{lcm}(x^{\ell_i} - 1)$. The last diagonal block of $\mathrm{RCF}(T)$ is the companion matrix for $m_T(x)$, so if this polynomial is not of the form $x^m - 1$, then $\mathrm{RCF}(T)$ will not be a permutation matrix.

(Solution begins here!) So, a counterexample is given by $\tau = (1\ 2)(3\ 4\ 5)$, which has the properties that $\chi_T(x) = (x^2 - 1)(x^3 - 1)$ and $m_T(x) = \mathrm{lcm}(x^2 - 1, x^3 - 1) = x^4 + x^3 - x - 1$. The invariant factors must be $(x - 1), (x^4 + x^3 - x - 1)$, and the rational canonical form is

$$
\mathrm{RCF}(T) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{bmatrix},
$$

which is not a permutation matrix. (Solution ends here.)

The discussion above shows that $\mathrm{RCF}(T)$ is a permutation matrix iff τ can be written as a product of disjoint cycles of lengths $\ell_1, \ldots, \ell_k$ where $\ell_1 | \cdots | \ell_k$.

Group 2.

3. Find the rational canonical form and the Jordan canonical form of

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

Solution. Since $A - I$ has a zero row, 1 must be an eigenvalue for A. Let's investigate the Jordan blocks associated to eigenvalue 1.

If $B := A - I$, then $B \neq 0$ and $B^2 = 0$. This proves that the minimal polynomial of B is x^2, so its invariant factors are either x, x, x^2 or x^2, x^2. Since B has rank 2, they are x^2, x^2. (The other choice would force $\mathrm{rk}(B) = \mathrm{rk}(\mathrm{RCF}(B)) = 1$.) Hence the invariant factors of A are $(x-1)^2, (x-1)^2$. These are prime powers, so they are also the elementary divisors. It follows from this that

$$\mathrm{RCF}(A) = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{bmatrix}, \qquad \mathrm{JCF}(A) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

.

4. Show that the functor $V \mapsto V^*, \varphi \mapsto \varphi^*$ is an exact functor from the category of $\mathbb{F}$-spaces to itself.

(Discussion) $V \mapsto V^*$ is a hom functor, hom functors are additive, and additive functors preserve split exact sequences. Thus, it is enough to observe that any exact sequence $0 \to U \xrightarrow{f} V \xrightarrow{g} W \to 0$ of $\mathbb{F}$-spaces splits. (End discussion.)

Solution 1. Choose a complement W' of $f(U)$ in V. Then $g|_{W'}\colon W' \to W$ is an isomorphism, so $s = (g|_{W'})^{-1}$ is a section of g (meaning $s\colon W \to V$ and $gs = id_W$). Exact sequences with a section are split.

Solution 2. All vector spaces are free, hence projective. But if W is projective, then the sequence splits.

Solution 3. All vector spaces are injective. But if U is injective, then the sequence splits.

Group 3.

5. Let R be the subring of $\mathbb{Q}$ whose elements are $\left\{\dfrac{m}{n} \in \mathbb{Q} \mid n \text{ odd}\right\}$. R is a PID. Describe the finitely generated torsion R-modules, and show that that are finite.

Solution. R is an integral domain, since it is a subring of $\mathbb{Q}$. Every fraction m/n with odd numerator and denominator is a unit in R, so every element of R is an associate of a power of 2. This shows that every ideal is of the form (2^k) (hence R is a PID). A finitely generated torsion module is therefore of the form $R/(2^{i_1}) \oplus \cdots \oplus R/(2^{i_r})$.

Claim. $\overline{\overline{\varphi}}\colon \mathbb{Z}_{2^k} = \mathbb{Z}/(2^k) \to R/(2^k)\colon \bar{z} \to \bar{z}$ is a ring isomorphism.

Let $\overline{\varphi}$ be the composition of the unique ring homomorphism $\varphi\colon \mathbb{Z} \to R$ with the natural map $\nu\colon R \to R/(2^k)$. This homomorphism has kernel $(2^k) \subseteq \mathbb{Z}$, so the induced map $\overline{\overline{\varphi}}\colon \mathbb{Z}/(2^k) \to R/(2^k)$ is a ring embedding. If $m/n \in R$, then the congruence $nx \equiv m \pmod{2^k}$ is solvable in $\mathbb{Z}$, since $\gcd(n, 2^k) = 1$. This means that there exist $x, y \in \mathbb{Z}$ such that $nx = m + 2^k y$, or $x = m/n + 2^k y/n$ in $\mathbb{Q}$, or $x = m/n + (2^k)$ in R. This shows that every element $m/n \in R$ is congruent to an element $x \in \varphi(\mathbb{Z})$ modulo (2^k), so $\overline{\overline{\varphi}}$ is surjective.

Now, the R-module structure on $R/(2^k)$ is determined by a ring homomorphism $R \to \mathrm{End}_{\mathbb{Z}}(R/(2^k))\colon r \mapsto \lambda_r$, and this homomorphism has kernel $\mathrm{Ann}_R(R/(2^k)) = (2^k)$, so it factors $R \xrightarrow{\nu} R/(2^k) \xrightarrow{\rho} \mathrm{End}_{\mathbb{Z}}(R/(2^k))$ where ρ is the regular representation.

Replacing $R/(2^k)$ by the isomorphic ring Z_{2^k} yields that the R module structure of R on $R/(2^k)$ is isomorphic to the R-module structure on $\mathbb{Z}_{2^k}$ given by

$$R \xrightarrow{\overline{\overline{\varphi}}^{-1}\circ\nu} \mathbb{Z}_{2^k} \xrightarrow{\rho'} \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_{2^k}),$$

where ρ' describes the regular representation of $\mathbb{Z}_{2^k}$. Examining the maps yields that R acts on $\mathbb{Z}_{2^k}$ via $(m/n)\bar{z} = \bar{m} \cdot \bar{n}^{-1} \cdot \bar{z}$ in the ring $\mathbb{Z}_{2^k}$.

We have fully described the addition and scalar multiplication of R on a cyclic torsion module, and a general f.g. torsion module is a finite direct sum of cyclic ones. The arguments show that any such module has size that is a finite power of 2.

6. Let R be an integral domain. For an R-module M and an element $r \in R$, let $M[r] = \{m \in M \mid rm = 0\}$. Show that the mapping $M \mapsto M[r]$ is the object part of a representable functor from the category of R-modules to itself.

Solution. Let F be the name of the functor mentioned. It suffices to find an R-module A and, for each R-module M, an R-module isomorphism $\eta_M \colon \mathrm{Hom}_R(A, M) \to F(M) = M[r]$. Then F can be defined on morphisms $\varphi\colon M \to N$ by $F(\varphi) = \eta_N \circ \varphi_* \circ \eta_M^{-1}$. This will automatically make F a functor and (η_M) a natural isomorphism from $\mathrm{Hom}_R(A, \_\!\_)$ to F.

The desired module is just $A = \langle a \mid ra = 0\rangle = R/(r)$. It follows from the universal property of presentations that the functions in $\mathrm{Hom}_R(A, M)$ are in 1-1 correspndence with the elements in M that satisfy the relation $rx = 0$. It is easy to check that the module operations correspond, so the function $\eta_M \colon \mathrm{Hom}_R(A, M) \to M[r]$ that maps a function φ to its value at a, $\varphi(a)$, is the desired isomorphism.

(In fact, the restriction of a homomorphism $\varphi\colon M \to N$ to the submodule $M[r]$ maps it into $N[r]$, and $F(\varphi) = \eta_N \circ \varphi_* \circ \eta_M^{-1}$ turns out to be $\varphi|_{M[r]}$.)