1. **Exact sequences** A sequence of $R$-module maps $A \xrightarrow{\phi} B \xrightarrow{\pi} C$ is **exact** if the kernel of $\pi$ and the image of $\phi$ are the exact same submodule of $B$. A longer sequence is exact by definition if every subsequence of two consecutive maps is exact.

a). Show that $B \xrightarrow{\pi} C \rightarrow 0$ is exact if and only if $\pi$ is surjective.

The kernel of $C \rightarrow 0$ is all of $C$, so it is exact if the image of $\pi$ is all of $C$—that is, if $\pi$ is surjective.

b). Show that $0 \rightarrow A \xrightarrow{\phi} B$ is exact if and only if $\phi$ is injective.

The image of $0 \rightarrow A$ is zero, so the kernel of $\phi$ should be 0 for this to be exact, that is, $\phi$ should be injective.

c) The sequence $A \xrightarrow{\phi} B \rightarrow C \rightarrow 0$ is exact if and only the map $B \rightarrow C$ is surjective and has kernel the image of $\phi$. By the first isomorphism theorem, this says $C$ is isomorphic to the cokernel of $\phi$.

d). The sequence $0 \rightarrow A \rightarrow B \xrightarrow{\pi} C$ is exact if and only if the map $A \rightarrow B$ is injective and its image is kernel $\pi$.

e). The first isomorphism theorem for $R$-modules says that if $\phi : B \rightarrow C$ is a surjective, then $C \cong B/\ker \phi$. This expressed by the exact sequence $0 \rightarrow \ker \phi \rightarrow B \xrightarrow{\phi} C \rightarrow 0$.

f). Given two modules $M$ and $N$, show that there is an five-term exact sequence $0 \rightarrow M \rightarrow M \oplus N \rightarrow N \rightarrow 0$.

The projection $M \oplus N$ onto $N$ has kernel $M \oplus 0$ in $M \oplus N$. This is expressed by $0 \rightarrow M \rightarrow M \oplus N \rightarrow N \rightarrow 0$, where the first non-trivial map sends $m \mapsto (m,0)$.

Find an example of a five-term exact sequence $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ in which $B$ is not isomorphic to $A \oplus C$ [in fact, this is much more typical than the case $B \cong A \oplus C$, except of course in the very special case where $R$ is a field.]

Many examples work: $0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$ where the first non-trivial arrow is “multiplication by 2.”

2. **Modules of Homomorphisms.** If $M$ and $N$ are $R$-modules over a commutative ring, denote by $\text{Hom}_R(M, N)$ the set of all $R$-module homomorphisms $M \rightarrow N$. 

a). Prove that $\text{Hom}_R(M, N)$ has a natural $R$-module structure. Give an example to show that this is false for non-commutative $R$.

The additive structure is easy: $f + g$ sends $m$ to $f(m) + g(m)$, which is another $R$-linear additive map from $M$ to $N$. This is easily seen to be an additive group structure on $\text{Hom}_R(M, N)$, with zero the zero map. Also, we can define $rf$ to be the function sending $m$ to $rf(m)$. This is still additive, and it is $R$ linear if $R$ is commutative: note that for $s \in R$, we need to check that for all $m$, $rf(sm) = sr(f(m)$, but since $f$ is $R$-linear, this is the same as $rsf(m) = sr(f(m)$, which is true if $rs = sr$.

Let $R$ be a non-commutative ring in which $rs \neq sr$ for some $r, s$. Given $\phi \in \text{Hom}_R(M, N)$, we want $rf$ (however it is defined) to be $R$-linear, so that for all $x \in M$, we have $rf(sx) = sr(f(x)$. But $f$ is $R$-linear, so this means we need $rsf(x) = sr(f(x)$ for all $x \in M$. It is easy to cook up examples where this fails. For example, say $M = N = R$. Then the identity map $\iota : M \to M$ sends $x = 1$ to $1$. But then $rsf(x) \neq sr(f(x)$ since $rs \cdot 1 \neq sr \cdot 1$. For a specific example, let $R = D$ be the Weyl algebra $\mathbb{R}[x, \frac{d}{dx}]$, let $R = x$ and $s = \frac{d}{dx}$.

b). Describe explicitly all $\mathbb{Z}$-module maps $\mathbb{Z}/(30) \to \mathbb{Z}/(21)$.

We essentially did this in class: any such map is determined by the image of the generator $\bar{1}$. In order for the map to be well-defined, this must go to something in $\mathbb{Z}/(21)$ killed by $30$. The options are the classes of $0, 7$ and $14$.

c). Prove that $\text{Hom}_\mathbb{Z}(\mathbb{Z}/(n), \mathbb{Z}/(m)) \cong \mathbb{Z}/(m, n)$. [Remember: you need an explicit map in order to prove two objects are isomorphic.]

A map in $\text{Hom}_\mathbb{Z}(\mathbb{Z}/(n), \mathbb{Z}/(m))$ is determined by the image of $\bar{1}$, which can go to any class $\bar{d}$ such that $m \bar{d} \bar{n}$ (otherwise it is not well-defined). The set of possible $d$ is an ideal of $\mathbb{Z}$, so it must be principal, say generated by $d_0$. Call this map $\phi_{d_0}$, and note then that $\text{Hom}_\mathbb{Z}(\mathbb{Z}/(n), \mathbb{Z}/(m))$ is a cyclic $\mathbb{Z}$-module generated by $\phi_{d_0}$. In fact, it is not hard to see that $d_0 = \frac{m}{(m, n)}$ (using the UFD property of $\mathbb{Z}$). So there is a surjective $\mathbb{Z}$-module map $\Psi : \mathbb{Z} \to \text{Hom}_\mathbb{Z}(\mathbb{Z}/(n), \mathbb{Z}/(m))$ sending $1$ to the map $\phi_{d_0}$. We need only prove the kernel is $(m, n)$. This is the same as saying that the annihilator of $\phi_{d_0}$ is $(m, n)$. But $(m, n)\phi_{d_0}$ sends $\bar{1}$ to the class of $(m, n)d_0 = (m, n)\frac{m}{(m, n)} = m$, which is zero, and no proper factor of $(m, n)$ does the same. By the first isomorphism theorem, there is an induced isomorphism $\mathbb{Z}/(m, n) \to \text{Hom}_\mathbb{Z}(\mathbb{Z}/(n), \mathbb{Z}/(m))$.

d) Observe that the category of $R$-modules has the following features: both the image and the kernel of a map of $R$-modules are $R$-modules, and all morphism sets $\text{Mor}(M, N)$ (denoted $\text{Hom}_R(M, N)$ in this category) has a natural abelian group structure. These are the main features of an Abelian Category. Which of the following seven categories shares these features; $\text{Grp}, \text{Ab}, \text{CommRing}, \text{Vect}_k$ ($k$-vector spaces), smooth manifolds, $\text{Top}$, or $\text{Set}$?

Only $\text{Ab}$, and $\text{Vect}_k$ share these features. The category $\text{Grp}$ does not always have cokernels (since not all subgroups are normal). The category $\text{CommRing}$ does not have kernels (since the kernel of a ring map is an ideal, not a subring). The categories of smooth manifolds, $\text{Top}$, and $\text{Set}$ have no natural way of adding maps, so no natural group structure on the
morphism sets.

3. Let $V$ be the five dimensional $\mathbb{R}$-vector space of polynomials of degree four or less in one variable.\(^1\) Consider this as a $\mathbb{R}[x]$-module where $x$ acts by differentiation. Using the structure theory for modules over a PID, express $V$ as a direct sum of cyclic $\mathbb{R}[x]$-modules. What are the invariant factors?

Let $V$ be the $\mathbb{R}$-vector space spanned by $1, t, t^2, t^3, t^4$ (a subspace of $\mathbb{R}[t]$). The operator $\frac{d}{dt}$ makes this into a cyclic $\mathbb{R}[x]$-module, generated by $t^4$. Note that $(\frac{d}{dt})^5$ is zero, but $(\frac{d}{dt})^4$ is not, so the minimal polynomial is $x^5$. Since $V$ is five dimensional, we have an $\mathbb{R}[x]$-module isomorphism $V \cong \mathbb{R}[x]/x^5$.

4. Find the cardinality of the set of all distinct (non-isomorphic) $\mathbb{F}_p[x]$-module structures on $\mathbb{F}_p^2$.

Using the invariant factor decomposition, this is the same as counting the different invariant factors. There are either two of degree one (which are the same) or one of degree 2. There are $p$ possibilities in the first case, where the invariant factors are both $x - a$ for $a \in \mathbb{F}_p$. There are $p^2$ possibilities in the second case, where the invariant factor is $x^2 - ax - b$ for $a, b \in \mathbb{F}_p$. The total is $p^2 + p$.

5. Up to similarity, find the complete list of all $6 \times 6$ matrices over $\mathbb{Q}$ whose minimal polynomial is divisible by $x^2(x - 1)^2$.

The minimal polynomial could have degree four, five or six. If degree is four, then it is $x^2(x - 1)^2$. There additional invariant factors: either one of dimension two or two of dimension one. In the former case, these would be either $x, x$ or $x - 1, x - 1$. In the latter case there are three possibilities: $x^2, (x - 1)^2$, or $x(x - 1)$. Thus we have a total of five $6 \times 6$ matrices whose minimal polynomial is $x^2(x - 1)^2$, up to similarity. These are the block matrices made of companion matrices for the five sequences of invariant factors: $\{x, x, x^2(x - 1)^2\}, \{x - 1, x - 1, x^2(x - 1)^2\}, \{x^2, x^2(x - 1)^2\}, \{(x - 1)^2, x^2(x - 1)^2\}$, and $\{x(x - 1), x^2(x - 1)^2\}$.

If the degree of the minimal polynomial is five, then $m(x) = x^2(x - 1)^2(x - a)$ for some $a \in \mathbb{Q}$. In this case, there is exactly one more invariant factor, which is necessarily of the form $(x - b)$ where $b = 0, 1$ or $a$. Thus the similarity classes are represented by $6 \times 6$ block matrices: a $1 \times 1$ block 'b', with a $5 \times 5$ the companion matrix of $m(x)$. This is essentially a one-parameter family, parametrized by $a$, but for each $a$ there are three possible values for the $1 \times 1$-block, so it is a “three-sheeted cover of a one-parameter family.”

If the degree of the minimal polynomial is six, then $m(x) = x^2(x - 1)^2(x^2 + cx + d)$, and the module is cyclic. Theses matrices are companion matrices for $m$. There is a two-parameter family of them over $\mathbb{Q}$.

6. Let $R = k[x]$ where $k$ is field. Let $V$ be any $R$-module. Consider the $k$-vector space homomorphism $T : V \to V$ sending $v$ to $x \cdot v$.

\(^1\)My advice is to name this variable something other than $x$. 

3
a). Prove that a $T$-stable subspace of the vector space $V$ and is the same as an $R$-submodule of the $R$-module $V$. [Recall from linear algebra that a subspace $W$ of $V$ is $T$-stable if $T(W) \subset W$.]

Say $W \subset V$ is $T$-stable. Then it is also an $k[x]$-submodule, since is a abelian subgroup $V$ (being a sub-vectorspace), and $T(W) \subset W$ implies $T^j(W) \subset W$ for all $j$, so that $W$ is closed under the action of any polynomial $f \in k[x]$. Conversely, if $W$ is a $k[x]$-submodule, then it is closed under $k[x]$, in a particular $x \cdot W \subset W$, so $T(W) \subset W$.

b). If $V$ is finitely dimensional over $k$, prove that its annihilator in $R$ is generated by the minimal polynomial of $T$.

The annihilator of $V$ is principal, say generated by monic $g \in k[x]$. Then $g(x)$ kills every element of $V$, which means $g(x) \cdot v = 0$ for all $v \in V$. Thus $g(T)$ is the zero operator on $V$. Conversely, if $h$ also acts by zero, then $h(T)$ kills every element of $V$, which means $h(x)$ is in the annihilator of $V$. The smallest degree monic polynomial with this property is the minimal polynomial (by definition). But also ideals in $k[x]$ are generated by the lowest degree monic member.

c). Show that $V$ is a cyclic $R$-module if and only if there exists an element $v$ such that the vectors $v, T(v), T^2(v), T^3(v) \ldots$ span $V$ as a $k$ vector space.

An $R$ module $V$ is cyclic if and only if it is generated some $v \in V$. Thus every element in $V$ is of the form $f(x) \cdot v$ for some $f$. But this is $f(T)v$, which is a linear combination of the $T^j(v)$. Conversely, if the $v, T(v), T^2(v), T^3(v) \ldots$ span $V$ as a $k$ vector space, then every $w \in V$ can be written $a_0v + a_1T(v) + a_2T^2(v) + a_3T^3(v) \ldots a_nT^n(v)$. So then $w = f(x) \cdot v$, where $f = a_0 + a_1x + a_2x^2 + \ldots a_nx^n$.

d). Prove that $\lambda$ is an eigenvalue for $T$ if and only if there is an non-zero element $v$ in $V$ which is annihilated by the polynomial $x - \lambda$. Describe an $R$-module presentation for the $R$-submodule of $V$ generated by $v$.

An element $\lambda$ is an eigenvalue if there exists non-zero $v \in V$ such that $T(v) = \lambda v$. But then $(x - \lambda)$ kills $v$. The submodule generated by $v$ is presented by $k[x]/(x - \lambda)$.

e). Let $V$ be the $R$-module $k[x]/(x - a)^n$. Prove that there are exactly $n$-non-zero $R$-submodules of $V$ and that they are linearly ordered by inclusion. Show that there is exactly one one-dimensional $T$-stable subspace of the $k$-vector space $V$. Find a generator (i.e., an element of $k[x]/(x - a)^n$) for this subspace when considered as an $R$-module via the bijection in part a.

The $T$-stable submodules are the $k[x]$-submodules of $k[x]/(x - a)^n$, which are in 1-1 correspondence with the submodules of $k[x]$ (ideals) containing $(x - a)^n$. An ideal containing $(x - a)^n$ is generated by an element $g$ dividing $(x - a)^n$, so by the UFD property of $k[x]$, it must be of the form $(x - \lambda)^j$ for some $j \leq n$. These are the linearly ordered submodules, generated by the classes of $(x - \lambda)^j$ as $j$ goes from $n$ (the zero module) to 0 (the whole module $k[x]/(x - a)^n$).

f). Let $V$ be finite dimensional. Characterize what it means for $T$ to be diagonalizable in terms of a decomposition of $V$ into cyclic $R$-modules.
It means that $V$ has a presentation by cyclic modules of the form $k[x]/(x - a)$.

g. Assume $V$ is finite dimensional over $k$, and has a basis $v_1, \ldots, v_n$ of eigenvectors. Using these as $R$-module generators, find the corresponding matrix presenting $V$ as a surjective image of $R^n$.

We did this in class: the matrix is diagonal with entries $(x - \lambda_i)$ ranging through the eigenvalues (with multiplicities).

7. Fix a domain $R$. For any $R$-module, let $End_R(M)$ denote the set of $R$-module homomorphisms from $M$ to itself.

a). Show that $End_R(M)$ has a natural ring structure and that its group of units is the set $Aut_R(M)$ of $R$-module self-isomorphisms of $M$.

We have done this before: composition is the multiplication, and we define addition by usual function addition (add the outputs). The identity map is the multiplicative identity. If $\phi : M \to M$ is invertible, this exactly means that there exists a $\psi : M \to M$ such that $\phi \circ \psi$ and $\psi \circ \phi$ are the identity maps, i.e., they are units in $End_R(M)$.

b). In the case $M = R^n$, show that $End_R(M)$ is isomorphic to the ring of $n \times n$ matrices with coefficients in $R$, and that $Aut_R(M)$ is the subset of matrices whose determinant is in $R^*$. [You may interpret “determinant” here as over the fraction field of $R$ if you haven’t since the determinant of a matrix over a ring before.]

We have seen already that a map $R^n \to R^n$ is given by matrix multiplication (on the left) with composition of maps corresponding to matrix multiplication. If $R^n \to R^n$ is an automorphism (say given by multiplication by matrix $A$), then there exists an inverse map given by $B$ such that $A \circ B$ and $B \circ A$ are the identity matrix. But since $R \subset F$, its fraction field, we can view these matrices as matrices over $F$ as well, and see then then $\det(A)\det(B) = \det(AB) = 1$. Note that the formula for the determinant is polynomial in the entries of $A$ and $B$, so these determinants are in $R$. But also their product is 1, so they are units in $R$.

8. Let $R$ be a Euclidean domain, and let $A$ be an $m \times n$ matrix with entries in $R$.

a). Show that after a series of invertible elementary row and column operations, we can assume that the matrix has zeros in the first rows/column except in position 11. [Hint: try putting/keeping the smallest entry in the 11 position.]

Done in class. First permute so we can assume $a_{11}$ has minimal value of $\delta$ among all entries. Then use division algorithm to replace entry $a_{12}$ by either zero or some remainder $r$ of value less than $a_{11}$ (this is done by replacing column two $C_2$ by $C_2 - qC_1$ where $a_{12} = a_{11}q + r$ as in the division algorithm. Now, repeat again, putting smallest value into 11-position. Continuing in this way, we eventually clear out the first row, then column (except in the 11-spot).

b). Show that any matrix over a Euclidean domain can be diagonalized after a series of row/column operations. [Hint: induce.]

Use induction on the size of the matrix, min $\{m, n\}$. If $m$ or $n$ is one, the argument above
makes it all zeros except the first entry. Otherwise, the argument above can be used to make
the matrix block form: the $a_{11}$ entry is non-zero, but the $(m - 1) \times (n - 1)$ matrix below is
smaller, so can be diagonalized by induction. Those operations don’t touch the first row or
column, since they don’t involve the non-zero part.

c). Show that if $B$ is obtained from $A$ by a series of column operations, then $B = AQ$ where
$Q$ is an invertible $n \times n$ matrix over $R$.

We did this in class: invertible column ops correspond to multiplication by an invertible
elementary matrix (obtained by doing that same column op on the $n \times n$ identity matrix) on
the right. A sequence of these is a multiplication by the corresponding product of elementary
matrices, which is necessarily invertible.

d). Show that if $B$ is obtained from $A$ by a series of row operations, then $B = PA$ where $P$
is an invertible $m \times m$ matrix over $R$.

Ditto, with rows instead of columns and left instead of right.