1. Let R be an integral domain and let M be an R-module. Give the definition of each of the following terms:

   (a) M is a *free* R-module.

   ▶ **Solution.** The R-module M if free if it has a basis. (Page 129) ◀

   (b) M is a *cyclic* R-module.

   ▶ **Solution.** M is cyclic if it is generated by a single element. (Page 115) ◀

   Now determine if each of the following statements about R-modules is true or false. Give a proof or counterexample, as appropriate.

   (a) A submodule of a free module is free.

   ▶ **Solution. False.** Let $M = R$. Then M is a free R-module (with basis $\{1\}$). If I is any ideal of R that is not principal, then I is a submodule that is not free since any two distinct nonzero elements of I are linearly dependent: $ba + (-a)b = 0$. Thus a basis would have to have 1 element, but I is not principal. For a concrete example, let $R = \mathbb{Z}[X]$ and $I = \langle 2, X\rangle$. ◀

   (b) A submodule of a cyclic module is cyclic.

   ▶ **Solution. False.** The same example as in part (a) works. ◀

   (c) A quotient module of a free module is free.

   ▶ **Solution. False.** Let $R = M = \mathbb{Z}$. Then $\mathbb{Z}_2$ is a quotient module of M that is not free. ◀

   (d) A quotient module of a cyclic module is cyclic.

   ▶ **Solution. True.** Suppose that $M = \langle m\rangle$ is cyclic and $\pi : M \to N$ is a surjective R-module homomorphism, i.e., N is a quotient of N. Then $N = \langle \pi(m)\rangle$ so N is cyclic. ◀

2. List without repetition all of the abelian groups of order $72 = 3^2 2^3$.

   ▶ **Solution.** All abelian groups of a given order $m = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ can be described uniquely in elementary divisor form by listing the distinct ways of writing each r_i as a sum of nondecreasing natural numbers ≥ 1. Since $72 = 2^3 \cdot 3^2$ we get $p_1 = 2$, $r_1 = 3$, $p_2 = 3$, $r_2 = 2$.

Abelian Groups of order 72

Exponent Partition		Group
$r_1 = 3$	$r_2 = 2$	Elementary Divisor Form
3	2	$\mathbb{Z}_{2^3} \times \mathbb{Z}_{3^2}$
$2+1$	2	$\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2}$
$1+1+1$	2	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2}$
3	$1+1$	$\mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_3$
$2+1$	$1+1$	$\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$
$1+1+1$	$1+1$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

◀

Identify which group on your list is isomorphic to each of the following groups.

(a) $\mathbb{Z}_{72}$ **Answer:** $\mathbb{Z}_{2^3} \times \mathbb{Z}_{3^2}$

(b) $\mathbb{Z}_4 \times \mathbb{Z}_{18}$ **Answer:** $\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2}$

(c) $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_6$ **Answer:** $\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

3. Let $K \subseteq \mathbb{Z}^3$ be the $\mathbb{Z}$-submodule generated by $v_1 = (1, 0, -1)$ and $v_2 = (5, 6, 7)$.

(a) Find a basis $\{x_1,\ x_2,\ x_3\}$ of $\mathbb{Z}^3$ and integers s_1 and s_2, with $s_1 | s_2$, so that $\{s_1x_1,\ s_2x_2\}$ is a basis of K.

▶ **Solution.** If $\mathcal{B} = \{e_1 = (1, 0, 0),\ e_2 = (0, 1, 0),\ e_3 = (0, 0, 1)\}$ is the standard basis of $\mathbb{Z}^3$, then the relation matrix for the generators v_1, v_2 with respect to $\mathcal{B}$ is $A = \begin{bmatrix} 1 & 0 & -1 \\ 5 & 6 & 7 \end{bmatrix}$. By row and column operations, compute the Smith normal form of A:

$$QAP^{-1} = \begin{bmatrix} 1 & 0 \\ -5 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & -1 \\ 5 & 6 & 7 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 6 & 0 \end{bmatrix} = D.$$

This gives a matrix identity $QA = DP$, i.e.,

$$QA = \begin{bmatrix} 1 & 0 \\ -5 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & -1 \\ 5 & 6 & 7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 6 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix} = DP.$$

Since P is invertible, its rows form a basis of $\mathbb{Z}^3$ so let $x_1 = (1, 0, -1)$, $x_2 = (0, 1, 2)$, and $x_3 = (0, 0, 1)$. Then the matrix equation gives $x_1 = v_1$, $6x_2 = -5v_1 + v_2$ so $\{x_1,\ 6x_2\}$ is a basis of K so we may take $s_1 = 1$, $s_2 = 6$. ◀

(b) What is the order of each of the elements $x_i + K$ in the quotient group $\mathbb{Z}^3/K$?

▶ **Solution.** Since $x_1 \in K$, $x_1 + K = 0 \in \mathbb{Z}^3/K$ so it has order 0. Moreover, $6x_2 \in K$ so the order of $x_2 + K$ is 6, and since $\langle x_3 \rangle \cap K = \langle 0 \rangle$, it follows that no multiple of x_3 is in K, so the order of x_3 is infinite. ◀

(c) Determine the structure of $\mathbb{Z}^3/K$ as a direct sum of cyclic submodules.

► **Solution.** Letting $\overline{x_i} = x_i + K \in \mathbb{Z}^3/K$, it follows from the above calculations that $\mathbb{Z}^3/K = \mathbb{Z}\overline{x_2} \oplus \mathbb{Z}\overline{x_3}$ so that $\mathbb{Z}^3/K \cong \mathbb{Z}_6 \oplus \mathbb{Z}$. ◄

4. Let V be a vector space over the real numbers $\mathbb{R}$ and let $T : V \to V$ be a linear transformation. Describe how V can be made into an $\mathbb{R}[X]$-module (denoted V_T) via T.

► **Solution.** The scalar multiplication is defined by $f(X)v = f(T)(v)$ for all $f(X) \in \mathbb{R}[X]$. ◄

Suppose that V has a basis $\mathcal{B} = \{e_1, e_2, e_3\}$ and T is the linear transformation defined by $T(e_1) = 2e_1$, $T(e_2) = -4e_2 - 4e_3$, and $T(e_3) = 9e_2 + 8e_3$.

(a) Compute the matrix representation $[T]_\mathcal{B}$.

► **Solution.**

$$[T]_\mathcal{B} = \begin{bmatrix} 2 & 0 & 0 \\ 0 & -4 & 9 \\ 0 & -4 & 8 \end{bmatrix}.$$

◄

(b) Calculate $(X-2)e_1$ and $(X-2)^2e_2$. **Answer:** Both are 0.

(c) Show that $V_T = \mathbb{R}[X]e_1 \oplus \mathbb{R}[X]e_2$.

► **Solution.** Since $T(e_1) = 2e_1$ it follows that $\mathbb{R}[X]e_1$ is the $\mathbb{R}$-subspace of V with basis e_1. Moreover, since $T(e_2)$ and $T(e_3$ are both $\mathbb{R}$-linear combinations of e_2 and e_3, it follows that the $\mathbb{R}[X]$-submodule generated by e_2 is contained in the 2 dimensional subspace of V with basis $\{e_2, e_2\}$ and since $T(e_2)$ is not a scalar multiple of e_2, it follows that

$$\mathbb{R}[X]e_2 = \{be_2 + ce_3 : b, c \in \mathbb{R}\}.$$

Thus, V is the vector space direct sum of the T-invariant subspaces $V_1 = \langle e_1 \rangle$ and $V_2 = \langle e_2, e_3 \rangle$ so that

$$V_T = V_1 \oplus V_2 = \mathbb{R}[X]e_1 \oplus \mathbb{R}[X]e_2.$$

◄

(d) What are the invariant factors of T?

► **Solution.** From Part (b) we see that $\mathrm{Ann}(e_1) = \langle X-2 \rangle$ and $\mathrm{Ann}(e_2) = \langle (X-2)^2 \rangle$. Then the direct sum cyclic decomposition in part (c) shows that the invariant factors of V_T are $f_1(X) = X - 2$, and $f_2(X) = (X-2)^2$. ◄

(e) Find the Jordan canonical form J of T and a basis $\mathcal{C}$ for V such that $[T]_\mathcal{C} = J$.

▶ **Solution.** From part (d), we see that the Jordan canonical form is

$$J = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix}.$$

From the proof of the Jordan canonical form theorem we see that a basis $\mathcal{C} = \{v_1, v_2, v_3\}$ for V such that $[T]_{\mathcal{C}} = J$ is given by $v_1 = e_1$, $v_3 = e_2$, and $v_2 = (X-2)e_2 = -6e_2 - 4e_3$. ◀

5. Let $A \in M_n(\mathbb{R})$ be a real matrix such that $A^2 = I_n$. Describe all possible Jordan canonical forms for the matrix A.

▶ **Solution.** Since $A^2 = I_n$ it follows that $f(A) = 0$ for the quadratic polynomial $f(X) = X^2 - 1 = (X+1)(X-1)$. It follows that the minimal polynomial $m_A(X)$ must divide $X^2 - 1$, so that $m_A(X)$ is one of the three polynomials $X - 1$, $X + 1$, or $X^2 - 1$. In case $m_A(X) = X - 1$, then $A = I_n$, and in case $m_A(X) = X + 1$, then $A = -I_n$. In case $m_A(X) = X^2 - 1$ then $m_A(X)$ factors into distinct linear factors, and hence A is diagonalizable, i.e., the Jordan form is $I_k \oplus -I_{n-k}$ for $1 \le k \le n-1$. Thus one can express the Jordan form as a diagonal matrix with k copies of 1 on the diagonal and $n - k$ copies of -1 for $0 \le k \le n$. ◀