Please, remember to write your name. There are five questions in total. Answers not accompanied by reason will receive no credit, even if they are correct. We write $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ to denote the ring of rational integers, rational numbers, and real numbers, respectively. For any rational prime $p$, we write $\mathbb{F}_p$ to denote the finite field $\mathbb{Z}/p\mathbb{Z}$. **Good luck and show your work.**

<table>
<thead>
<tr>
<th>Problem</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
</tr>
<tr>
<td>D</td>
<td></td>
</tr>
<tr>
<td>E</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
</tr>
</tbody>
</table>
A. (20 points)

Let $A$ be any $\mathbb{Z}$-module. Prove that $\text{Hom}_\mathbb{Z}(\mathbb{Z}/n\mathbb{Z}, A) \simeq A_n$, where

$$A_n = \{a \in A : na = 0\}.$$

Let $\Phi : \text{Hom}_\mathbb{Z}(\mathbb{Z}/n\mathbb{Z}, A) \longrightarrow A_n$ be the map given by $\Phi(f) = f(\bar{1})$. (Note that $nf(1) = f(\bar{n}) = 0$.) It is straightforward to check that $\Phi$ is $\mathbb{Z}$-linear.

$\Phi$ is one-to-one: Suppose $\Phi(f) = 0$, i.e., $f(\bar{1}) = 0$. Then $f(x) = x \cdot f(\bar{1}) = 0$, for any $x \in \mathbb{Z}$. Thus $f = 0$.

$\Phi$ is onto: Say $a \in A_n$. Put $f(\bar{x}) = xa$. This is well defined since, if $\bar{x} = \bar{y}$, then $(x - y)a = 0$. It is clear that $f$ is $\mathbb{Z}$-linear, and that $\Phi(f) = a$. 
B. (15 points)

Prove that every finite abelian group is a torsion $\mathbb{Z}$-module. Give an example of an infinite abelian group that is not a torsion $\mathbb{Z}$-module.

Let $n$ be the order of the group. Let us write the group additively and we will assume that it is not the trivial group. Hence $n > 1$, and $nx = 0$ for any non-trivial $x$ in the group. Thus it is a torsion $\mathbb{Z}$-module. $\mathbb{Z}$ is an infinite abelian group that is not torsion.
C. (20 points)

Let $R$ be a PID and let $M$ and $N$ be free $R$ modules of the same finite rank. Prove that an $R$-module homomorphism $f : M \rightarrow N$ is an injection if and only if $N/\text{Im}(f)$ is a torsion $R$-module.

Let $n$ be the rank of $M$ and $N$ respectively. Suppose $f$ is an injection, then $f(M) \subset N$ is a submodule of $N$ of rank $n$. Hence there exists a basis $\{x_1, x_2, \ldots, x_n\}$ of $M$ so that $\{a_1x_1, a_2x_2, \ldots, a_nx_n\}$ is a basis of $f(M)$, where $a_1, a_2, \ldots, a_n$ are nonzero elements of $R$ satisfying $a_1/a_2/\ldots/a_n$. Thus

$$N = Rx_1 \oplus Rx_2 \oplus \cdots \oplus Rx_n$$
$$f(M) = Ra_1x_1 \oplus Ra_2x_2 \oplus \cdots \oplus Ra_nx_n,$$

and therefore

$$N/f(M) \simeq R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_n).$$

In fact one can check that the map $\sum b_ix_i \mapsto \sum b_i(\text{mod}(a_i))$ from $N \rightarrow R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_n)$ factors through $f(M)$ and yields the desired isomorphism.

Conversely, if $N/f(M)$ is torsion, then $f(M)$ should have the same rank as that of $N$, i.e., $n$. On the other hand we also know that (over a PID) $\text{rank(Im}f) + \text{rank(ker}f) = n$. Thus the rank of ker$f$ is 0, which implies ker$f = 0$. Thus $f$ is an injection.
D. (20 points)

Let \( R = \mathbb{R}[X] \) and suppose that \( M \) is a direct sum of cyclic \( R \)-modules with annihilators \((X - 1)^3, (X^2 + 1)^2, (X - 1)(X^2 + 1)^4\), and \((X + 2)(X^2 + 1)^2\). Determine the elementary divisors and invariant factors of \( M \).

It is given that

\[
M \simeq \mathbb{R}/(X - 1)^3 \oplus \mathbb{R}/(X^2 + 1)^2 \oplus \mathbb{R}/(X - 1)(X^2 + 1)^4 \oplus \mathbb{R}/(X + 2)(X^2 + 1)^2
\]

Since \( X^2 + 1 \) is irreducible over \( \mathbb{R} \), using the Chinese remainder theorem and uniqueness of elementary divisors, we see that the elementary divisors of \( M \) are

\[
(X - 1)^3, (X^2 + 1)^2, (X - 1), (X^2 + 1)^4, (X + 2), (X^2 + 1)^2
\]

We can recover the invariant factors of \( M \). Namely \( a_3(X) = (X - 1)^3(X^2 + 1)^4(X + 2) \), \( a_2(X) = (X - 1)(X^2 + 1)^2 \), and \( a_1(X) = (X^2 + 1)^2 \). Note \( a_1(X)/a_2(X)/a_3(X) \).
E. (20 points)

Determine up to similarity all $3 \times 3$ invertible matrices over $\mathbb{F}_2$.

The minimal polynomial is of degree 1, 2 or 3. Let us consider each of these cases. Let $R$ be the rational canonical form of $A$. Keep in mind that $-1 = 1$ in $\mathbb{F}_2$.

(a). $m_A(x) = x^3 + ax^2 + bx + c$. Then $m_A(x) = c_A(x)$, and $R$ is just the companion matrix of $m_A(x)$, i.e.,

$$ R = \begin{pmatrix} 0 & 0 & -c \\ 1 & 0 & -b \\ 0 & 1 & -a \end{pmatrix} $$

Since $a, b, c \in \mathbb{F}_2 = \{0, 1\}$, and $\det(A) \neq 0$, we see that $R$ should be one of the following

$$ \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} $$

(b). $m_A(x) = x^2 + bx + c$. Then the other invariant factor is linear, say of the form $x - a$, with $(x - a)(x^2 + bx + c)$ being the characteristic polynomial of $A$, and $x - a$ should divide $x^2 + bx + c$. Since $\det(A) \neq 0$, we see that the only possibility is that $m_A(x) = x^2 + 1$, and $c_A(x) = (x + 1)^3$. Hence $R$ is given by

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

(c). $m_A(x) = x - 1$. Then all the invariant factors are linear and equals $x - 1$. Hence $R$ is

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

These are all the $3 \times 3$ matrices up to similarity.