**Math 202 - Assignment 7**

Authors: Yusuf Goren, Miguel-Angel Manrique and Rory Laster

**Proposition 1** ([DE], p342). Let $R$ be a ring and let $M$ be an $R$-module. A subset $N$ of $M$ is an $R$-submodule of $M$ if and only if

1. $N$ is nonempty and
2. $x + ry \in N$ for all $r \in R$ and all $x, y \in N$.

**Exercise 10.1.4.** Let $R$ be a ring with identity, let $M$ be the $R$-module $R^n$ with component-wise addition and multiplication, and let $I_1, I_2, \ldots, I_n$ be left ideals of $R$ for some $n \in \mathbb{N}$. The following are submodules of $R^n$:

a. $N_1 = \{(i_1, i_2, \ldots, i_n) : i_k \in I_k \text{ for all } k \in \{1, 2, \ldots, n\}\}$

b. $N_2 = \{(x_1, x_2, \ldots, x_n) : \sum_{k=1}^n x_k = 0\}$.

**Proof.** To prove (a), it suffices to show, by Proposition 1, that $N_1$ is nonempty and $x + ry \in N_1$ for all $r \in R$ and all $x, y \in N_1$. For the first condition, $(0, 0, \ldots, 0) \in N_1$ since $I_k$ is a subgroup of $R$ containing the additive identity 0 for all $k \in \{1, 2, \ldots, n\}$. That is, $N_1$ is nonempty.

For the second condition, let $x = (i_k)_{k \in \mathbb{Z}^+}, y = (y_k)_{k \in \mathbb{Z}^+} \in N_1$ and let $r \in R$. Then, by definition of addition and scalar multiplication,

$$x + ry = (i_k)_{k \in \mathbb{Z}^+} + r(y_k)_{k \in \mathbb{Z}^+} = (i_k + ry_k)_{k \in \mathbb{Z}^+} \in N_1,$$

since $i_k + ry_k \in I_k$ for all $k \in \{1, 2, \ldots, n\}$ by the left ideal axioms. This gives us (a).

To establish (b), we apply a similar method as that used in (a). Since $\sum_{k=1}^n 0 = 0$, the element $(0, 0, \ldots, 0) \in N_2$. Thus $N_2$ is nonempty. Moreover if $x = (i_k)_{k \in \mathbb{Z}^+}, y = (y_k)_{k \in \mathbb{Z}^+} \in N_1$ and $r \in R$, then

$$x + ry = (i_k)_{k \in \mathbb{Z}^+} + r(y_k)_{k \in \mathbb{Z}^+} = (i_k + ry_k)_{k \in \mathbb{Z}^+}.$$

Therefore, because

$$\sum_{k=1}^n x_k + ry_k = \sum_{k=1}^n x_k + r \left( \sum_{k=1}^n y_k \right) = 0 + r0 = 0,$$

we have that $x + ry \in N_2$ by definition.

**Exercise 10.1.5.** Let $R$ be a ring with identity, let $I$ be a left ideal of $R$ and let $M$ be a left $R$-module. Define

$$IM := \left\{ \sum_{\text{finite}} a_i m_i : a_i \in I \text{ and } m_i \in M \text{ for all } i \right\}.$$

$IM$ is an $R$-submodule of $M$. 

Proof. It suffices to show, by Proposition 1, that $IM$ is nonempty and $x + ry \in IM$ for all $r \in R$ and all $x, y \in IM$. For the former condition, observe that $0_R \in I$ since $I$ is an additive subgroup of $R$ and $0_M \in M$ because $M$ is a group. Hence the finite sum $0_R \cdot 0_M = 0_M$ satisfies the membership condition of $IM$. Therefore $IM$ is nonempty.

For the latter condition, let $r \in R$ and let $x = \sum_{i=1}^n a_i m_i, y = \sum_{i=1}^m a'_i m'_i \in IM$ such that $n, m \in \mathbb{N}$, $a_i, a'_i \in I$ and $m_i, m'_i \in M$. Then

$$x + ry = \sum_{i=1}^n a_i m_i + r \cdot \left( \sum_{i=1}^m a'_i m'_i \right)$$

$$= \sum_{i=1}^n a_i m_i + \sum_{i=1}^m (ra'_i) m'_i$$

$$= \sum_{i=1}^n a_i m_i + \sum_{i=1}^m a''_i m'_i$$

for $a''_i = ra'_i \in I$. That is, $x + ry$ is a finite sum of elements of the form $am$ such that $a \in I$ and $m \in M$. Thus $x + ry \in IM$.

Exercise 10.1.6. Let $R$ be a ring with identity and let $M$ be a left $R$-module. For any nonempty collection $\{N_i\}_{i \in I}$ of $R$-submodules of $M$, the intersection

$$N = \bigcap_{i \in I} N_i$$

is an $R$-submodule of $M$.

Proof. Observe that $N$ is a subset of $M$ since, for all $n \in N$, $n$ is an element of some $N_i$ with $i \in I$. Hence $n \in M$. So it suffices to show, by Proposition 1, that $N$ is nonempty and $x + ry \in N$ for all $r \in R$ and all $x, y \in N$. For the first property, $0_M \in N_i$ for all $i \in I$ because each $N_i$ is an additive subgroup of $M$. Therefore $0_M \in N = \cap_{i \in I} N_i$ and, so, $N$ is nonempty.

For the second property, let $r \in R$ and let $x, y \in N$. Then $x$ and $y$ are elements of $N_i$ for all $i \in I$ by definition. Thus, by the submodule axioms, $x + ry \in N_i$ for each $i \in I$. That is, $x + ry \in N = \cap_{i \in I} N_i$.

Exercise 10.1.7. Let $R$ be a ring with identity and let $M$ be a left $R$-module. If $N_1 \subseteq N_2 \subseteq \ldots$ is an ascending chain of $R$-submodules of $M$, then

$$N = \bigcup_{i=1}^{\infty} N_i$$

is an $R$-submodule of $M$ as well.

Proof. Suppose that $N_1 \subseteq N_2 \subseteq \ldots$ is an ascending chain of $R$-submodules of $M$. To prove that $N$ is also an $R$-submodule of $M$, it suffices to show, by Proposition 1, that $N$ is nonempty and that $x + ry \in N$ for all $r \in R$ and all $x, y \in N$.

Since $0 \in N_1$, $0$ is an element of the union $N$. Hence $N$ is nonempty. For the remaining property, let $r \in R$ and let $x, y \in N$. Because $x$ and $y$ are elements of $N$, each must be an element of a submodule. That is, $x \in N_j$ and $y \in N_k$ for some $j, k \in \mathbb{N}$. By the ascending chain hypothesis, $N_{\min(j,k)} \subseteq N_{\max(j,k)}$. Therefore both $x$ and $y$ are members of $N_{\max(j,k)}$. Moreover, by the submodule axioms, $x + ry \in N_{\max(j,k)}$. Hence, since $N_{\max(j,k)} \subseteq N$, we have that $x + ry \in N$.

Definition. Let $R$ be a ring and let $M$ be a left $R$-module. A torsion element is an element $m \in M$ such that $rm = 0$ for some nonzero $r \in R$. 
Definition. Let $R$ be an integral domain and let $M$ be a left $R$-module. The set

$$\text{Tor}(M) = \{ m \in M : m \text{ is a torsion element} \}$$

is the torsion submodule of $M$.

Exercise 10.1.8. Let $R$ be a ring with identity and let $M$ be a left $R$-module.

a. If $R$ is an integral domain, then $\text{Tor}(M)$ is an $R$-submodule of $M$.

b. there exists a ring $R$ with identity and a left $R$-module $M$ such that $\text{Tor}(M)$ is not a submodule of $M$ and

c. if $R$ has zero divisors, then every nonzero left $R$-module contains nonzero torsion elements.

Proof. To prove (a), we suppose that $R$ is an integral domain. It suffices to show, by Proposition 1, that $\text{Tor}(M)$ is nonempty and $x + ry \in \text{Tor}(M)$ for all $x, y \in \text{Tor}(M)$ and all $r \in R$.

For the former condition, $0 \in \text{Tor}(M)$ since $1 \cdot 0 = 0$. Hence $\text{Tor}(M)$ is nonempty. For the final condition, let $x, y \in \text{Tor}(M)$ and let $r \in R$. As torsion elements, there exist nonzero $s, t \in R$ such that $s \cdot x = 0$ and $t \cdot y = 0$. Thus

$$(st) \cdot (x + ry) = (st) \cdot x + [(st)r] \cdot y$$

by the $R$-module axioms

$$= (ts) \cdot x + [(sr)t] \cdot y$$

by the commutativity of $R$

$$= t \cdot (s \cdot x) + (sr) \cdot (t \cdot y)$$

by the $R$-module axioms

$$= t \cdot 0 + (sr) \cdot 0$$

since $s \cdot x = 0$ and $t \cdot y = 0$

$$= 0.$$

Because $R$ is an integral domain and $s, t$ are nonzero, the product $st$ is nonzero. Therefore, we have shown that $(st) \cdot (x + ry) = 0$ for a nonzero $st \in R$. That is, $x + ry \in \text{Tor}(M)$ and (a) is immediate.

To see that (b) holds, consider the ring $R = M = \mathbb{Z}/6\mathbb{Z}$ and the elements $\overline{2}, \overline{3} \in R$. $R$ is a left $R$-module with respect to addition and left ring multiplication. Moreover, since

$$\overline{2} \cdot \overline{3} = \overline{6} = 0$$

and

$$\overline{3} \cdot \overline{2} = \overline{6} = 0,$$

we find that $\overline{2}$ and $\overline{3}$ are elements of $\text{Tor}(M)$. However, since $\overline{2} + \overline{3} = \overline{5} \notin \text{Tor}(M)$, $M$ is not closed under addition. That is, $\text{Tor}(M)$ is not a subgroup of $M$ and, hence, it is not a submodule of $M$ either. Thus there exists a ring $R$ and $R$-module $M$ with the desired properties.

For (c), suppose that $R$ contains the zero divisors $s$ and $r$ such that $sr = 0$. Then, for any nonzero left $R$-module $M$ with nonzero element $m$, either $r \cdot m = 0$ or $r \cdot m \neq 0$. In the first case of $r \cdot m = 0$, $m \in \text{Tor}(M)$ since $r$ is nonzero by hypothesis. In the second case of $r \cdot m \neq 0$, we find that $r \cdot m \in \text{Tor}(M)$ because

$$s \cdot (r \cdot m) = (sr) \cdot m$$

by the $R$-module axioms

$$= 0 \cdot m$$

by hypothesis

$$= 0.$$

In either case, there exists a nonzero element contained in $\text{Tor}(M)$. This is the desired result. □

Definition. Let $R$ be a ring with identity and let $M$ be a left $R$-module. The annihilator of a submodule $N$ of $M$ is the set

$$\text{Ann}(N) = \{ r \in R : r \cdot n = 0 \text{ for all } n \in N \}.$$

**Exercise 10.1.9.** Let $R$ be a ring with identity and let $M$ be a left $R$-module. For any $R$-submodule $N$ of $M$, the annihilator of $N$ in $R$ is a two-sided ideal of $R$.

**Proof.** Suppose that $N$ is an $R$-submodule of $M$. It suffices to show that $Ann(N)$ is nonempty and that $x + rys \in Ann(N)$ for all $x, y \in Ann(N)$ and all $r, s \in R$. For the former condition, consider the element $0_R$. Since

$$0_R \cdot n = 0_N$$

for any $n \in N$, we see that $0_R \in Ann(N)$.

For the remaining condition, we let $x, y \in Ann(N)$ and let $r, s \in R$. For any $n \in N$, we have that

$$(x + rys) \cdot n = x \cdot n + r \cdot (y \cdot (s \cdot n))$$

by the $R$-module axioms

$$= 0 + r \cdot 0$$

since $x, y \in Ann(N)$ and $sn \in N$

$$= 0.$$

Hence $x + rys \in Ann(N)$. 

**Definition.** Let $R$ be a ring with identity and let $M$ be a left $R$-module. The annihilator of an ideal $I$ of $R$ is the set

$$Ann(I) = \{ m \in M : i \cdot m = 0 \text{ for all } i \in I \}.$$

**Exercise 10.1.10.** Let $R$ be a ring with identity and let $M$ be a left $R$-module. For any ideal $I$ of $R$, $Ann(I)$ is an $R$-submodule of $M$.

**Proof.** Suppose that $I$ is an ideal of $R$. To prove the desired result, it suffices to show, by Proposition 1, that $Ann(I)$ is nonempty and $x + ry \in Ann(I)$ for all $x, y \in Ann(I)$ and all $r \in R$.

To see that $Ann(I)$ is nonempty, observe that

$$i \cdot 0_N = 0_N$$

for all $i \in I$. Thus $0_N \in Ann(I)$.

For the remaining condition, let $x, y \in Ann(I)$ and let $r \in R$. If $i \in I$, then $ir \in I$ by the ideal axioms. Hence

$$i \cdot (x + ry) = i \cdot x + (ir) \cdot y$$

by the $R$-submodule axioms

$$= 0 + 0$$

since $x, y \in Ann(I)$ and $ir \in I$

$$= 0.$$

Therefore $x + ry \in Ann(I)$. 

**Exercise 10.1.11.** Let $M$ be the $\mathbb{Z}$-module $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$.

a. $Ann(M) = 600\mathbb{Z}$ and

b. $Ann(2\mathbb{Z}) \cong G \times H$ such that $G = \langle 12 + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 0 + 50\mathbb{Z} \rangle$ and $H = \langle 0 + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 25 + 50\mathbb{Z} \rangle$.

**Proof.** For (a), we appeal to the definition of set equality. To see the first inclusion, let $a \in Ann(M)$. As it annihilates all elements of $M$, $a$ must annihilate $(1 + 24\mathbb{Z}, 1 + 15\mathbb{Z}, 1 + 50\mathbb{Z}) \in M$. That is,

$$0 = a \cdot (1 + 24\mathbb{Z}, 1 + 15\mathbb{Z}, 1 + 50\mathbb{Z}) = (a + 24\mathbb{Z}, a + 15\mathbb{Z}, a + 50\mathbb{Z}).$$

Since $0 = (0 + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 0 + 50\mathbb{Z})$, the previous equation implies that

$$\begin{cases} a + 24\mathbb{Z} = 0 + 24\mathbb{Z}, \\
a + 15\mathbb{Z} = 0 + 15\mathbb{Z} \mbox{ and} \\
a + 50\mathbb{Z} = 0 + 50\mathbb{Z}. \end{cases}$$

For (b), we have

$$Ann(2\mathbb{Z}) \cong G \times H$$

where $G = \langle 12 + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 0 + 50\mathbb{Z} \rangle$ and $H = \langle 0 + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 25 + 50\mathbb{Z} \rangle$. 

**Exercise 10.1.12.** Let $M$ be a left $R$-module.

a. $Ann(M) = 0$ and

b. $Ann(2\mathbb{Z}) \cong G \times H$ such that $G = \langle 12 + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 0 + 50\mathbb{Z} \rangle$ and $H = \langle 0 + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 25 + 50\mathbb{Z} \rangle$. 

**Proof.** For (a), we appeal to the definition of set equality. To see the first inclusion, let $a \in Ann(M)$. As it annihilates all elements of $M$, $a$ must annihilate $(1 + 24\mathbb{Z}, 1 + 15\mathbb{Z}, 1 + 50\mathbb{Z}) \in M$. That is,

$$0 = a \cdot (1 + 24\mathbb{Z}, 1 + 15\mathbb{Z}, 1 + 50\mathbb{Z}) = (a + 24\mathbb{Z}, a + 15\mathbb{Z}, a + 50\mathbb{Z}).$$

Since $0 = (0 + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 0 + 50\mathbb{Z})$, the previous equation implies that

$$\begin{cases} a + 24\mathbb{Z} = 0 + 24\mathbb{Z}, \\
a + 15\mathbb{Z} = 0 + 15\mathbb{Z} \mbox{ and} \\
a + 50\mathbb{Z} = 0 + 50\mathbb{Z}. \end{cases}$$
Hence $a \in 24\mathbb{Z} \cap 15\mathbb{Z} \cap 50\mathbb{Z} = 600\mathbb{Z}$.

For the opposite inclusion, let $a \in 600\mathbb{Z}$. Because 24, 15 and 50 are divisors of 600, observe that $ab$ is an element of each of $24\mathbb{Z}$, $15\mathbb{Z}$ and $50\mathbb{Z}$ for any $b \in \mathbb{Z}$. Therefore, for all $(x+24\mathbb{Z}, y+15\mathbb{Z}, z+50\mathbb{Z}) \in M$,

\[
a \cdot (x + 24\mathbb{Z}, y + 15\mathbb{Z}, z + 50\mathbb{Z}) = (ax + 24\mathbb{Z}, ay + 15\mathbb{Z}, az + 50\mathbb{Z}) = (0 + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 0 + 50\mathbb{Z}) = 0.
\]

Thus $a$ annihilates all elements of $M$ and, consequently, $a \in \text{Ann}(M)$ and we have now shown that $\text{Ann}(M) = 600\mathbb{Z}$. This is (a).

For (b), we proceed similarly to the argument given in (a). To demonstrate the first inclusion, let $a = (x + 24\mathbb{Z}, y + 15\mathbb{Z}, z + 50\mathbb{Z}) \in \text{Ann}(2\mathbb{Z})$. Then $a$ annihilates all elements of $2\mathbb{Z}$ and, in particular, $a$ annihilates 2. Thus

\[
0 = 2 \cdot a = 2 \cdot (x + 24\mathbb{Z}, y + 15\mathbb{Z}, z + 50\mathbb{Z}) = (2x + 24\mathbb{Z}, 2y + 15\mathbb{Z}, 2z + 50\mathbb{Z})
\]

That is, we have the system of linear congruences

\[
\begin{align*}
2x & \equiv 0 \pmod{24}, \\
2y & \equiv 0 \pmod{15}, \\
2z & \equiv 0 \pmod{50}.
\end{align*}
\]

By elementary number theoretic results, this system is equivalent to

\[
\begin{align*}
x & \equiv 0 \pmod{12}, \\
y & \equiv 0 \pmod{15}, \\
z & \equiv 0 \pmod{25}.
\end{align*}
\]

Therefore $x = 12x’, y = 15y’$ and $z = 25z’$ for some $x’, y’, z’ \in \mathbb{Z}$. Moreover,

\[
(x + 24\mathbb{Z}, y + 15\mathbb{Z}, z + 50\mathbb{Z}) = (12x’ + 24\mathbb{Z}, 15y’ + 15\mathbb{Z}, 25z’ + 50\mathbb{Z}) = (12x’ + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 25z’ + 50\mathbb{Z}) = (12x’ + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 0 + 50\mathbb{Z}) + (0 + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 25z’ + 50\mathbb{Z}) \in G + H.
\]

Hence $\text{Ann}(2\mathbb{Z}) \subseteq G + H$.

For the opposite inclusion, let $a \in G + H$. Then

\[
a = n \cdot (12 + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 0 + 50\mathbb{Z}) + m \cdot (0 + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 25 + 50\mathbb{Z}) = (12n + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 0 + 50\mathbb{Z}) + (0 + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 25m + 50\mathbb{Z})
\]

for some $n, m \in \mathbb{Z}$. For any element $i$ in the ideal $2\mathbb{Z}$, it follows that $i = 2j$ for some $j \in \mathbb{Z}$. Thus

\[
i \cdot a = (2j) \cdot [(12n + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 0 + 50\mathbb{Z}) + (0 + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 25m + 50\mathbb{Z})] = (2j) \cdot (12n + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 0 + 50\mathbb{Z}) + (2j) \cdot (0 + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 25m + 50\mathbb{Z})] = (24jn + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 0 + 50\mathbb{Z}) + (0 + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 50jm + 50\mathbb{Z})] = (0 + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 0 + 50\mathbb{Z}) + (0 + 24\mathbb{Z}, 0 + 15\mathbb{Z}, 0 + 50\mathbb{Z})] = 0.
\]

Hence $a$ annihilates all elements of $2\mathbb{Z}$ and, therefore, $a \in \text{Ann}(2\mathbb{Z})$. This establishes the opposite inclusion of $G + H \subseteq \text{Ann}(2\mathbb{Z})$ and, so, $\text{Ann}(2\mathbb{Z}) = G + H$. Furthermore, since $G \cap H = \{0\}$, it follows that $G + H \cong G \times H$ and, so, $\text{Ann}(2\mathbb{Z}) \cong G \times H$. □
**Exercise 10.1.14.** Let $R$ be a ring with identity and let $M$ be a left $R$-module. For any element $z$ of the center of $R$,

$$zM = \{zm : m \in M\}$$

is an $R$-submodule of $M$.

**Proof.** Let $z$ be an element of the center of $R$. It suffices to show, by Proposition 1, that $zM$ is nonempty and $x + ry \in zM$ for all $x, y \in zM$ and all $r \in R$. Since $0_M \in M$,

$$z \cdot 0_M = 0_M \in zM.$$  

That is, $zM$ is nonempty.

For the remaining submodule criterion, let $x = zm, y = zm' \in zM$ and let $r \in R$. Then

$$x + ry = z \cdot m + r \cdot (z \cdot m')$$

by the $R$-submodule axioms

$$= z \cdot m + (rz) \cdot m'$$

since $z$ is in the center of $R$

$$= z \cdot (m + r \cdot m')$$

by the $R$-submodule axioms.

Therefore, because $m + r \cdot m' \in M$, we have that $x + ry \in zM$.

**Corollary.** Let $R = M_2(F)$ for a field $F$ and let

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in M_2(F).$$

Then $e$ is not in the center of $R$.

**Proof.** Consider $R$ as a left $R$-module in the natural way. The element $e = e \cdot 1_R$ is a member of $R$ and, also,

$$r = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \in R.$$  

Since

$$re = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} = r$$

and $r \notin eR$, we find that $eR$ is not closed under scalar multiplication. Therefore $eR$ is not a submodule of $R$. This implies, by the contrapositive to Exercise 10.1.14, that $e$ is not in the center of $R$. 

**Exercise 10.1.16.** Let $V = F^n$ for a field $F$ and let $T : V \to V$ be the shift operator defined by

$$T(v_1, v_2, \ldots, v_n) = (v_2, \ldots, v_n, 0).$$

If we View $V$ as an $F[x]$-module with $x$ acting by the operator $T$ and if $U$ is an $F[x]$-submodule of $V$, then $U = U_k$ for some $U_k = \text{Span}\{e_i : 1 \leq i \leq k\}$ such that $k \in \{0, 1, \ldots, n\}$.

**Proof.** The abelian group $V = F^n$ is a left $F[x]$-module when endowed with a scalar multiplication

$$\cdot : F[x] \times V \to V$$

defined by

$$\left( \sum_{i=0}^{m} a_i x^i \right) \cdot v = \sum_{i=0}^{m} a_i T^i(v)$$

for all $\sum_{i=0}^{m} a_i x^i \in F[x]$ and all $v \in V$.

With this definition in mind, suppose that $U$ is an $F[x]$-submodule of $V$. There exists a maximal element in the set of integers

$$S = \{m \in \mathbb{Z} : \text{ there exists an element } u \in U \text{ such that } u \text{ has nonzero } m\text{th coordinate}\}$$

where
because there are only \( n \) coordinates in any element of \( V \). Let \( k \) be this maximal integer of \( S \). That is, for all \( u \in U \) and all \( l > k \), the \( l \)th coordinate of \( u \) is equal to 0.

We claim that \( U = U_k \) for this maximal \( k \). To see this, observe that \( U \) is closed under scalar multiplication by \( F[x] \) since it is a submodule. Hence, if \( f \) is a nonzero element in the \( k \)th coordinate of an element \( u = (u_1, \ldots, u_{k-1}, f, 0, \ldots, 0) \in U \), then

\[
(f^{-1}x^{k-1}) \cdot u = f^{-1}T^{k-1}(u) = f^{-1}(f, 0, \ldots, 0) = (1, 0, \ldots, 0) = e_1.
\]

Thus \( e_1 \in U \).

Furthermore, since \( U \) is also closed under addition,

\[
(f^{-1}x^{k-2}) \cdot u - (f^{-1}u_{k-1}) \cdot e_1 = f^{-1}T^{k-2}(u) - (f^{-1}u_{k-1}, 0, \ldots, 0) = f^{-1}(u_{k-1}, f, 0, \ldots, 0) - (f^{-1}u_{k-1}, 0, \ldots, 0) = (0, 1, 0, \ldots, 0) = e_2.
\]

So \( e_2 \in U \).

Continuing in this way, we find that \( e_i \in U \) for all \( i \in \{1, 2, \ldots, k\} \). Therefore \( \text{Span}(\{e_i : 1 \leq i \leq k\}) = U_k \) is contained in \( U \) by the \( F[x] \)-submodule properties. That is, \( U_k \subseteq U \). Moreover, since \( k \) is the maximal coordinate for which there is an element with nonzero entry, it follows that \( U \subseteq U_k \). Hence \( U = U_k \), as desired.

**Exercise 10.1.18.** Let \( F = \mathbb{R} \), let \( V = \mathbb{R}^2 \) and let \( T \in \text{End}_\mathbb{R}(V) \) be the map such that

\[
T(v) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \cdot v
\]

for all \( v \in V \). Then \( V \) and \( 0 \) are the only \( F[x] \)-submodules of \( V \) with respect to \( T \).

**Proof.** Let \( U \) be an \( F[x] \)-submodule of \( V \). Since \( F \) embeds into \( F[x] \), we may view \( V \) as an \( F \)-vector space and \( U \) as an \( F \)-subspace of \( V \). Either \( U = 0 \) or \( U = V \) or the dimension of \( U \) as an \( F \)-subspace is equal to 1. If \( \dim_{\mathbb{R}}(U) = 1 \), then there exists a nonzero element \( u \in U \) such that \( U = \text{span}_{\mathbb{R}}(u) \). For \( U \) to be an \( F[x] \)-submodule of \( V \), we must have that \( T(U) \subseteq U \) by the discussion in §10.1 of [DF]. In particular, \( T(u) = \lambda u \) for some \( \lambda \in F \). Therefore, by definition, \( u \) is an eigenvector of \( T \) with a real eigenvalue. However, the eigenvalues of \( T \) are \( \pm i \) and, so, \( T \) has no real eigenvalues. This contradiction implies that such a \( U \) cannot occur. That is, \( U = \{0\} \) or \( U = V \).

**Exercise 10.1.19.** Let \( F = \mathbb{R} \), let \( V = \mathbb{R}^2 \) and let \( T \in \text{End}_\mathbb{R}(V) \) be the map defined by \( T(a, b) = (0, b) \). Then the set

\[
S = \{W \subseteq V : W \text{ is an } F[x] \text{-submodule of } V\}
\]

satisfies \( S = \{0, W_x, W_y, V\} \) such that \( W_x = \{(a, 0) \in V : a \in \mathbb{R}\} \) and \( W_y = \{(0, b) \in V : b \in \mathbb{R}\} \).

**Proof.** The set of \( F[x] \)-submodules is equal to the set

\[
S = \{W \subseteq V : W \text{ is a subspace of } V \text{ and } W \text{ is } T\text{-stable}\}
\]

by an argument given in §10.1 of [DF].

For the subspace \( W_x \) of \( V \),

\[
T(a, 0) = (0, 0) \in W_x
\]

for all \( (a, 0) \in W_x \). Hence \( W_x \) is \( T \)-stable and, moreover, \( W_x \in S \).
Similarly, for the subspace $W_y$,

$$T(0, b) = (0, b) \in W_y$$

for all $(0, b) \in W_y$ and, consequently, $W_y \subseteq S$. It follows that, since $0$ and $V$ are trivially contained in $S$, $\{0, W_x, W_y, V\} \subseteq S$.

To demonstrate the opposite inclusion, we let $W \in S$. There are two cases of $W$: either $W$ contains an element $(a, b)$ such that both $a$ and $b$ are nonzero or it does not. In the first case of the existence of such an element $(a, b)$, we find that, by the $T$-stability of $W$,

$$T(u) = T(a, b) = (0, b) \in W.$$  

But $(a, b)$ and $(0, b)$ are $\mathbb{R}$-linearly independent since

$$\det \begin{pmatrix} a & b \\ 0 & b \end{pmatrix} = ab$$

and $a$ and $b$ are nonzero by hypothesis. Since it is a subspace of the two-dimensional $\mathbb{R}$-vector space $V$ containing two linearly independent elements, $W$ must equal $V$.

In the second case where no elements exist in $W$ of the form $(a, b)$ such that both $a$ and $b$ are nonzero, it follows that $W$ is either equal to $0$, $W_x$, or $W_y$. Thus $W \in\{0, W_x, W_y, V\}$, as desired. \qed

**Lemma 1.** Let $A$ be a $\mathbb{Z}$-module, let $a \in A$ and let $n$ be a positive integer. The map $\phi_a : \mathbb{Z}/n\mathbb{Z} \to A$ defined by $\phi_a(a) = ka$ is a well-defined $\mathbb{Z}$-module homomorphism if and only if $na = 0$.

**Proof.** Suppose that $\phi_a$ is a well-defined $\mathbb{Z}$-module homomorphism. In the $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$, $n \equiv 0$. Hence, because $\phi_a$ is well-defined,

$$na = \phi_a(n) = \phi_a(\bar{0}) = 0a = 0.$$

That is, $na = 0$.

For the converse statement, suppose that $na = 0$ and consider the map $\psi : \mathbb{Z} \to A$ defined by $\psi(k) = ka$ for all $k \in \mathbb{Z}$. This map is a group homomorphism since

$$\psi(k_1 + k_2) = (k_1 + k_2)a = k_1a + k_2a = \psi(k_1) + \psi(k_2)$$

for all $k_1, k_2 \in \mathbb{Z}$. Furthermore, because

$$\psi(nk) = \psi(kn) = (kn)a = k(na) = k\cdot 0 = 0$$

for all $nk \in n\mathbb{Z}$, we find that the subgroup $n\mathbb{Z}$ is contained in the kernel of $\psi$. Therefore $\psi$ descends to the quotient $\mathbb{Z}/n\mathbb{Z}$. That is, there exists a unique group homomorphism $\phi_a : \mathbb{Z}/n\mathbb{Z} \to A$ such that $\phi_a(a) = \psi(k) = ka$. Moreover, since

$$\phi_a(k_1 \bar{k_2}) = \phi_a(k_1 \bar{k_2}) = (k_1 k_2)a = k_1 (k_2 a) = k_1 \phi_a(k_2)$$

for all $k_1 \in \mathbb{Z}$ and all $\bar{k_2} \in \mathbb{Z}/n\mathbb{Z}$, it follows that $\phi_a$ is a $\mathbb{Z}$-module homomorphism. \qed
Exercise 10.2.4. Let $A$ be a $\mathbb{Z}$-module and let $n$ be a positive integer. Then $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A_n$ where $A_n = \{ a \in A : an = 0 \}$.

Proof. Let $\phi \in \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A)$ and let $a = \phi(1)$. For any $k \in \mathbb{Z}^+$, that $\phi$ is a $\mathbb{Z}$-module homomorphism implies

$$
\phi(k) = \phi \left( \sum_{i=1}^{k} 1 \right) = \sum_{i=1}^{k} \phi(1) = \sum_{i=1}^{k} a = \left( \sum_{i=1}^{k} 1 \right) a = ka.
$$

Thus $\phi = \phi_a$, with $\phi_a$ defined as in Lemma 1.

By Lemma 1, $\phi = \phi_a$ is a $\mathbb{Z}$-module homomorphism if and only if $na = 0$. Therefore the function $\psi : \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \to A_n$ defined by $\psi(\phi_a) = a$ is a bijection. Furthermore $\psi$ is a $\mathbb{Z}$-module homomorphism since

$$
\psi(a + a') = \psi(\phi_a + \phi_a') = \psi(\phi_{a+a'}) = a + a' = \psi(a) + \psi(a')
$$

and

$$
\psi(k\phi_a) = \psi(k\phi_a) = k\psi(\phi_a)
$$

for all $k \in \mathbb{Z}$ and all $\phi_a, \phi_a' \in \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A)$. That is, $\psi$ is an isomorphism and we have that $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A_n$.

Exercise 10.2.5. Let $a \in \mathbb{Z}/21\mathbb{Z}$ and let $\phi_a : \mathbb{Z}/30\mathbb{Z} \to \mathbb{Z}/21\mathbb{Z}$ denote the map defined by $\phi_a(1) = ka$. Then

$$
\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/30\mathbb{Z}, \mathbb{Z}/21\mathbb{Z}) = \{ \phi_7, \phi_{\overline{7}}, \phi_{\overline{11}} \}.
$$

Proof. By Exercise 10.2.4 the map $\psi : A_n \to \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/30\mathbb{Z}, \mathbb{Z}/21\mathbb{Z})$ defined by $\psi(\pi) = \phi_{\pi}$ is an isomorphism for $A_n = \{ \pi \in \mathbb{Z}/n\mathbb{Z} : 30\pi = 0 \}$. So it suffices to show that $A_n = \{ 0, \overline{7}, \overline{11} \}$.

For the set relation $A_n \subseteq \{ 0, \overline{7}, \overline{11} \}$, we let $\pi \in A_n$. Then

$$
30\pi = 30\overline{0} = 0 = \overline{0}
$$

(1)

since $\pi$ annihilates 30 by the membership condition of $A_n$. Thus, because $30\overline{a}$ and $\overline{0}$ are elements of $\mathbb{Z}/21\mathbb{Z}$, (1) implies that

$$
30\overline{a} \equiv 0 \pmod{21}.
$$

So, by definition, 21 divides 30 and there exists $b \in \mathbb{Z}$ such that $21b = 30a$. Dividing this equation by 3 yields that $7b = 10a$ and, because 7 is coprime to 10, we find that 7 must divide $a$. That is, $\pi \in \{ 0, \overline{7}, \overline{11} \}$.

For the opposite inclusion, we let $\pi \in \{ 0, \overline{7}, \overline{11} \}$. Then 7 divides $a$ and it is clear that, for some $b \in \mathbb{Z}$,

$$
30\overline{a} = 30\overline{7b} = 30 \cdot 7b = 21 \cdot 10b = \overline{0} = 0.
$$

Hence $\pi \in A_n$. Therefore $A_n = \{ 0, \overline{7}, \overline{11} \}$, as required.

Exercise 10.2.6. For all positive integers $m$ and $n$,

$$
\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/(n,m)\mathbb{Z}.
$$
Proof. Let $m$ and $n$ be positive integers. By Exercise 10.2.4

$$\text{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong A_n$$

where $A_n = \{ \bar{a} \in \mathbb{Z}/m\mathbb{Z} : na = 0 \}$. So it suffices to show that $A_n \cong \mathbb{Z}/(n,m)\mathbb{Z}$.

To see that this is the case, consider an arbitrary element $\bar{a} \in A_n$. As an element of $A_n$, $\bar{a}$ annihilates $n$ and, therefore,

$$\overline{na} = n\bar{a} = 0 = \overline{0}.$$ 

That is, $\overline{na} = \overline{0}$ in the group $\mathbb{Z}/m\mathbb{Z}$. Thus

$$na \equiv 0 \pmod{m}$$

to imply that there exists an integer $k$ such that $km = na$. Furthermore, we find by dividing by the greatest common divisor $(n,m)$ that

$$k \frac{m}{(n,m)} = \frac{n}{(n,m)}.$$ 

So $\frac{m}{(n,m)}$ divides the product $\frac{n}{(n,m)}a$. It follows, by elementary number theoretic results, that $\frac{m}{(n,m)}$ and $\frac{n}{(n,m)}$ must divide $a$. Since $a$ is divisible by $\frac{m}{(n,m)}$, $\bar{a} \in \left\{ \frac{km}{(n,m)} : 1 \leq k \leq (n,m) - 1 \right\}$.

Moreover, $A_n$ is isomorphic to $\mathbb{Z}/(n,m)\mathbb{Z}$ by the map $\phi: A_n \to \mathbb{Z}/(n,m)\mathbb{Z}$ defined by $\phi(\frac{km}{(n,m)}) = k$.

Exercise 10.2.9. Let $R$ be a commutative ring. Prove that $\text{Hom}_R(R,M)$ and $M$ are isomorphic as left $R$-modules.

Proof. Throughout this problem let $a, r, r' \in R$ and $m, m' \in M$. We follow the hint. Let $\varphi, \psi \in \text{Hom}_R(R, M)$. Suppose $\varphi(1) = \psi(1) = m$. We must have

$$\varphi(a \cdot 1) = a\varphi(1) = am$$
and

$$\psi(a \cdot 1) = a\psi(1) = am.$$