In class we defined (left) R-modules (p. 337); the exercises below will also require the definition of submodules of a left R-module (bottom of p. 337). In all the exercises, R denotes a ring with identity and M denotes a left R-module (which satisfies the condition (d) in the definition on page 337: $1_R \cdot m = m$ for every $m \in M$).

1. (Exercise 1 in DF §10.1.) Prove that $0m = 0$ and $(-1)m = -m$ for all $m \in M$.

Proof.
$$0m = (0+0)m = 0m + 0m,$$
therefore $0m$ is the additive identity. (In any group, if $gh = g$ for some g and some h, then h is the identity. Letting $g = h = 0m$ shows that $0m$ must be the identity in the additive group M.)
$$m + (-1)m = 1m + (-1)m = (1-1)m = 0m = 0,$$
therefore $(-1)m$ is the unique additive inverse $-m$ of m in M. □

2. (Exercise 4 in DF §10.1.) Let M be the left R-module R^n described in Example 3 on page 338. Let $I_1, \ldots, I_n$ be left ideals of R. Prove that the following are submodules of M:
   (a) $J = \{(x_1, x_2, \ldots, x_n) \in R^n : x_1 \in I_1, x_2 \in I_2, \ldots, x_n \in I_n\}$;
   (b) $Z = \{(x_1, x_2, \ldots, x_n) \in R^n : x_1 + x_2 + \ldots + x_n = 0\}$.

Proof. We will show that J and Z satisfy the submodule criterion given on pg. 342.

Let $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in J$, and $r \in R$. Any left ideal of R is a left R-module (this is part of example 1 on pg. 338), so $x_i + ry_i \in I_i$ for each i. Therefore, $x + ry = (x_1 + ry_1, \ldots, x_n + ry_n) \in J$. Clearly, J is nonempty since any ideal contains 0, so $(0, \ldots, 0) \in J$. Thus J is a submodule of M.

Z is nonempty because $0 + \cdots + 0 = 0$, so $(0, \ldots, 0) \in Z$. Let $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in Z$, and $r \in R$. Then
$$x_1 + ry_1 + \cdots x_n + ry_n = (x_1 + \cdots + x_n) + r(y_1 + \cdots + y_n) = 0 + r \cdot 0 = 0$$
so $x + ry \in Z$. Thus, Z is a submodule of M.

Note: We have used the fact here that $r \cdot 0 = 0$ for all $r \in R$. To prove this, assume that $r \cdot 0 = m \in M$. Then $r \cdot 0 = r \cdot (m - m) = r \cdot m + (-r) \cdot m = r \cdot m - r \cdot m = 0$. □

3. (Exercise 7 in DF §10.1.) Let $N_1, N_2, \ldots$ be an infinite sequence of submodules of M with $N_i \subset N_{i+1}$ for each $i \in \mathbf{N}$ (this is called an *ascending chain* of submodules of M). Prove that $\cup_{i=1}^{\infty} N_i$ is a submodule of M.

Proof. Since N_1 is a submodule of M, it contains 0. Thus $0 \in \cup_{i=1}^{\infty} N_i$, so this subset is nonempty.

Let $x, y \in \cup_{i=1}^{\infty} N_i$ and $r \in R$. Then there must be some i, j such that $x \in N_i$ and $y \in N_j$. Assume WLOG that $i \geq j$. Then $N_j \subset N_i$, thus $y \in N_i$ as well. So $x, y \in N_i$, thus $x + ry \in N_i \subset \cup_{i=1}^{\infty} N_i$ because N_i is a submodule. So $\cup_{i=1}^{\infty} N_i$ satisfies the submodule criterion. □

4. (Exercise 8 in DF §10.1.) An element m of the R-module M is called a *torsion element* if $rm = 0$ for some nonzero element $r \in R$. The set of torsion elements is denoted
$$\mathrm{Tor}(M) = \{m \in M : rm = 0 \text{ for some nonzero } r \in R\}.$$

   (a) Prove that if R is an integral domain, then $\mathrm{Tor}(M)$ is a submodule of M (called the *torsion submodule* of M). (Note that integral domains are assumed to be commutative.)

Proof. Suppose that R is an integral domain. Let $r \in R$ and $x, y \in \mathrm{Tor}(M)$, so that there exist some nonzero $a, b \in R$ such that $ax = by = 0$. Then ab is nonzero because R is an integral domain, and
$$ab(x + ry) = (ab)x + (abr)y = (ba)x + (arb)y = b(ax) + ar(by) = b(0) + ar(0) = 0 + 0 = 0.$$
Also, $\mathrm{Tor}(M)$ is nonempty since $1 \cdot 0 = 0$, and we are assuming that $1 \neq 0$ (as part of the definition of an integral domain). So $\mathrm{Tor}(M)$ satisfies the submodule criterion. □

(b) Give an example of a ring R and an R-module M such that $\text{Tor}(M)$ is not a submodule. [Hint: Consider the torsion elements in the R-module R.]

Proof. Let $R = \mathbb{Z}/6\mathbb{Z}$ and let M be R as a module over itself. Then $\text{Tor}(M) = \{0, 2, 3, 4\}$ since $0 = 1 \cdot 0 = 3 \cdot 2 = 2 \cdot 3 = 3 \cdot 4$, but 1 and 5 are relatively prime to 6 and so are not zero divisors. However, $2 + 3 = 5$ is not a torsion element, so $\text{Tor}(M)$ is not closed under addition. Thus, it is not a submodule of M. □

(c) If R has zero divisors, show that every nonzero R-module has nonzero torsion elements.

Proof. Assume that R has zero divisors, i.e. that there exist nonzero elements $a, b \in R$ such that $ab = 0$. Let M be a nonzero R-module, and suppose $m \in M$ is nonzero. If $bm = 0$, then m is a torsion element since b is nonzero. So assume that $bm \neq 0$. Then $a(bm) = (ab)m = 0m = 0$, thus bm is a nonzero torsion element because a is nonzero. □

5. (Exercise 11 in DF §10.1.) Let M be the abelian group (i.e., $\mathbf{Z}$-module—see the Example on p. 339) $\mathbf{Z}/24\mathbf{Z} \times \mathbf{Z}/15\mathbf{Z} \times \mathbf{Z}/50\mathbf{Z}$.

(a) Find the annihilator of M in $\mathbf{Z}$. (The annihilator of M is defined to be the subset $\{a \in \mathbf{Z} : ax = 0 \text{ for all } x \in M\}$. By Exercise 9 in §10.1 (which you may take for granted), the annihilator of M is an ideal of $\mathbf{Z}$; find a generator for it.)

Proof. The annihilator of M in $\mathbb{Z}$ is $600\mathbb{Z}$, which is the ideal generated by 600 in $\mathbb{Z}$ (note that 600 is the least common multiple of 24, 15, and 50).

First, check that $600\mathbb{Z}$ annihilates M. Any element of $600\mathbb{Z}$ is of the form $600z$ for some integer z. If (a, b, c) is any element of M, then $600z(a, b, c) = (24 \cdot 25a, 15 \cdot 40b, 50 \cdot 12c) = (0, 0, 0)$.

Next, check that $600\mathbb{Z}$ contains the annihilator of M in $\mathbb{Z}$. Suppose that $r \notin 600\mathbb{Z}$, so that $600 \nmid r$. We know that 600 divides any common multiple of $24, 15$, and 50, so one of these numbers does not divide r. Now, $(1, 1, 1) \in M$, but $r(1, 1, 1) = (r, r, r) \neq 0$ (if $24 \nmid r$ then the first component is nonzero, if $15 \nmid r$ then the second component is nonzero, and if $50 \nmid r$ then the third component is nonzero; we know that at least one of these is the case). So r is not in the anihilator of M in $\mathbb{Z}$, thus $600\mathbb{Z}$ contains the annihilator of M in $\mathbb{Z}$. □

(b) Let $I = 2\mathbf{Z}$. Describe the annihilator of I in M as a direct product of cyclic groups. (The annihilator of an ideal $I \subset \mathbf{Z}$ is defined to be the subset $\{x \in M : ax = 0 \text{ for all } a \in I\}$. By Exercise 10 in §10.1 (which you may take for granted), the annihilator of I is a submodule of M.)

Proof. Let $x = (a, b, c) \in M$. $rx = 0$ for all $r \in I$ if and only if $24 \mid ra$, $15 \mid rb$, and $50 \mid rc$ for all $r \in 2\mathbb{Z}$, or equivalently $24 \mid 2sa$, $15 \mid 2sb$, and $50 \mid 2sc$ for all $s \in \mathbb{Z}$.

$24 \mid 2sa$ for all $s \in \mathbb{Z}$ if and only if $a = 0$ or $a = 12$. $15 \mid 2sb$ for all $s \in \mathbb{Z}$ if and only if $b = 0$. $50 \mid 2sc$ if and only if $c = 0$ or $c = 25$. This means that the annihilator of I in M is the submodule

$$\{0, 12\} \times \{0\} \times \{0, 25\}.$$

Each of these groups are cyclic (each is isomorphic to either $\mathbb{Z}/2\mathbb{Z}$ or the trivial group), so this is a direct product of cyclic groups. □

6. (Exercise 15 in DF §10.1.) If M is a finite abelian group then M is naturally a $\mathbf{Z}$-module (cf. Example on p. 339). Can this action of $\mathbf{Z}$ on M be extended to make M into a $\mathbf{Q}$-module? (Prove your answer.)

The action of $\mathbb{Z}$ on M can be extended to make M into a $\mathbb{Q}$-module if and only if M is the trivial group.

Proof. Suppose $M = \{0\}$ is the trivial group. Then its structure as a $\mathbb{Z}$-module is defined by $r \cdot 0 = 0$ for all $r \in \mathbb{Z}$. This extends to a $\mathbb{Q}$-module by the definition $r \cdot x = 0$ for all $r \in \mathbb{Q}$. To check that both of these definitions satisfy the axioms of a module, let $r, s \in \mathbb{Q}$:

- $(r + s)0 = 0 = 0 + 0 = r(0) + s(0)$
- $(rs)0 = 0 = r(0) = r(s(0))$
- $r(0 + 0) = r(0) = 0 = 0 + 0 = r(0) + s(0)$

- $1(0) = 0$

Now, suppose that M is not the trivial group. Then M has some finite order $n > 1$, and it contains some non-identity element x. Denote the identity element of M by 0.

M is naturally a $\mathbb{Z}$-module, defined by some action $r \cdot m = rm$ for all $r \in \mathbb{Z}$, $m \in M$. Assume, for a contradiction, that this action can be extended to an action of $\mathbb{Q}$ on M, defined by $r \cdot m = rm$ for all $r \in \mathbb{Q}$. This requires that $\frac{1}{n}x = y$ for some $y \in M$. But then we have

$$x = \left(n\frac{1}{n}\right)x = n\left(\frac{1}{n}x\right) = ny = 0$$

(writing M multiplicatively instead, we have that $ny = y^n = 0$ because M has order n). This contradicts our assumption that x was not the identity element, thus such an extension does not exist when M is nontrivial. $\square$

7. (Exercise 21 in DF §10.1.) Let F be a field, and let $R = M_n(F)$ be the ring of $n \times n$ matrices with entries in F, where $n \in \mathbf{Z}_{\geq 2}$. Let M denote the set of matrices with arbitrary elements of F in the first column and zeros everywhere else; that is,

$$M = \{(c_{i,j}) \in R : c_{i,j} = 0 \ \forall \ j \neq 1\}.$$

Show that M is a submodule of R when R is considered as a left R-module, but M is not a submodule of R when R is considered as a right R-module.

(Note: an abelian group M has the structure of a right R-module if there is a map $R \times M \to M$, usually denoted $(r, m) \mapsto mr$, such that (a), (c), and (d) from the definition on page 337 hold, while (b) is replaced by the condition $m(rs) = (mr)s$. (If the map $R \times M \to M$ is written as $(r, m) \mapsto rm$, how should condition (b) be written?) In particular, just as the abelian group $M = R$ forms a left R-module via the map $R \times M \to M$ defined by $(r, m) \mapsto rm$ (where the operation in the expression rm is multiplication in R), it forms a right R-module via the map $R \times M \to M$ defined by $(r, m) \mapsto mr$.)

Proof. Let $B \in M$ and $A \in R$. The ijth entry of AB is the Euclidean inner product of the ith row of A with the jth column of B. Since the jth column of B is 0 for all $j > 1$, this means that the ijth entry of AB is 0 whenever $j > 1$, meaning that the only nonzero elements of AB are in the first column (where $j = 1$). Thus, $AB \in M$.

It is clear that M is closed under addition. If $A, B \in M$, then $a_{ij} = 0$ and $b_{ij} = 0$ whenever $j > 1$, so $a_{ij} + b_{ij} = 0$ whenever $j > 1$. It is also clear that M is nonempty, since it contains the 0 matrix. Therefore, M is a left submodule of R.

When R is considered as a right R-module, M is not a submodule because it is not closed under right multiplication by elements of R. Consider the matrices $A \in M$ and $B \in R$ where A has zeros in every entry except the top-left entry a_{11}, and B has zeros in every entry except the top-right entry b_{1n}. Then the first row of A is $\begin{pmatrix}1 & 0 & \cdots & 0\end{pmatrix}$ and the nth column of B is $\begin{pmatrix}1 & 0 & \cdots & 0\end{pmatrix}^T$. Therefore, the $1n$ entry of AB is

$$\begin{pmatrix}1 & 0 & \cdots & 0\end{pmatrix}\begin{pmatrix}1 & 0 & \cdots & 0\end{pmatrix}^T = 1,$$

so $AB \notin M$ (since $n \geq 2$). Thus M is not a right submodule of R. $\square$