Throughout \( R \) is a ring with unity.

Comment: It will become apparent that the module properties \( 0 \cdot m = 0, - (r m) = (-r) \cdot m \), and \( (r - r') \cdot m = r \cdot m - r' \cdot m \) are vital details in some problems.

1. \((20 \text{ total})\) Let \( M \) be an (additive) abelian group and \( \text{End}(M) \) be the set of group homomorphisms \( f : M \rightarrow M \).

(a) \((12)\) Show \( \text{End}(M) \) is a ring with unity, where \( (f + g)(m) = f(m) + g(m) \) and \( (fg)(m) = f(g(m)) \) for all \( f, g \in \text{End}(M) \) and \( m \in M \).

**Solution:** This is rather tedious, but not so unusual as a basic algebra exercise. The trick is to identify all of the things, large and small, which need to be verified.

We know that the composition of group homomorphisms is a group homomorphism. Thus \( \text{End}(M) \) is \textit{closed} under function composition. Moreover \( \text{End}(M) \) is a monoid since composition is an associative operation and the identity map \( I_M \) of \( M \) is a group homomorphism.

Let \( f, g, h \in \text{End}(M) \). The sum \( f + g \in \text{End}(M) \) since \( M \) is \textit{abelian} as

\[
(f + g)(m + n) = f(m + n) + g(m + n) \\
= f(m) + f(n) + g(m) + g(n) \\
= f(m) + g(m) + f(n) + g(n) \\
= (f + g)(m) + (f + g)(n)
\]

for all \( m, n \in M \). Thus \( \text{End}(M) \) is \textit{closed} under function addition.
Addition is commutative since \( f + g = g + f \) as \((f + g)(m) = f(m) + g(m) = g(m) + f(m) = (g + f)(m)\) for all \(m \in M\). In a similar manner one shows that addition is associative which boils down to \(((f + g) + h)(m) = (f + (g + h))(m)\) for all \(m \in M\).

We have seen from group theory that the zero function \(0 : M \rightarrow M\), defined by \(0(m) = 0\) for all \(m \in M\), is a group homomorphism. Thus \(0 \in \text{End}(M)\). The zero function serves as a neutral element for addition since function addition is commutative and \(f + 0 = f\) as \((f + 0)(m) = f(m) + 0(m) = f(m) + 0 = f(m)\) for all \(m \in M\).

Note that \(-f : M \rightarrow M\) defined by \((-f)(m) = -f(m)\) for all \(m \in M\) is a group homomorphism since

\[
(-f)(m + n) = -(f(m + n)) = -(f(m) + f(n)) = (-f(n)) + (-f(m)) = (-f(m)) + (-f(n)) = (-f)(m) + (-f)(n)
\]

for all \(m, n \in M\). The reader is left to show that \(-f\) is an additive inverse for \(f\). We have finally shown that \(\text{End}(M)\) is a group under addition.

To complete the proof that \(\text{End}(M)\) is a ring with unity we need to establish the distributive laws. First of all \(((f + g) \circ h)(m) = (f + g)(h(m))\) follows by definition of function composition and function addition since

\[
((f + g) \circ h)(m) = (f + g)(h(m)) = f(h(m)) + g(h(m)) = (f \circ h)(m) + (g \circ h)(m) = (f \circ h + g \circ h)(m)
\]

for all \(m \in M\). Since \(f\) is a group homomorphism the distributive law \(f \circ (g + h) = f \circ g + f \circ h\) holds as

\[
(f \circ (g + h))(m) = f((g + h)(m)) = f(g(m) + h(m))
\]
\[
\begin{align*}
&= f(g(m)) + f(h(m)) \\
&= (f \circ g)(m) + (f \circ h)(m) \\
&= (f \circ g + f \circ h)(m)
\end{align*}
\]

for all \( m \in M \). Therefore \( \text{End}(M) \) is a ring with unity.

**Comment:** The proof actually establishes more. For non-empty sets \( X, Y \) let \( \text{Fun}(X, Y) \) be the set of all functions \( f : X \to Y \).

Let \( M \) be a non-empty set. Then \( \text{Fun}(M, M) \) is a monoid under composition with neutral element \( I_M \).

Suppose that \( X \) is a non-empty set and \( M \) is an additive (not necessarily abelian) group. Then \( \text{Fun}(X, M) \), in particular \( \text{Fun}(M, M) \), is a group under function addition with neutral element the zero map \( 0 : X \to M \) defined by \( 0(x) = 0 \) for all \( x \in X \). Furthermore the distributive law

\[
(f + g) \circ h = f \circ h + g \circ h
\]

holds for all \( f, g, h, \in \text{Fun}(M, M) \).

Let \( f \in \text{Fun}(M, M) \) be fixed. Then the distributive law \( f \circ (g + h) = f \circ g + f \circ h \) holds for all \( g, h \in \text{Fun}(M, M) \) if and only if \( f \in \text{End}(M) \).

(To see this let \( m, n \in M \) and \( g(x) = m \) and \( h(x) = n \) for all \( x \in M \).)

Observe that \( \text{End}(M) \) is a submonoid of \( \text{Fun}(M, M) \) with neutral element \( I_M \). When \( M \) is abelian \( \text{End}(M) \) is a subgroup of \( \text{Fun}(M, M) \) under function addition. (In this case \( \text{End}(M) \) is a ring with unity under function addition and composition.)

Note that \( I_M + I_M \in \text{End}(M) \) if and only if \( M \) is abelian. Thus \( \text{End}(M) \) is closed under function addition if and only if \( M \) is abelian.

Now suppose that \( M \) is a left \( R \)-module.

(b) (8) For \( r \in R \) define \( \sigma_r : M \to M \) by \( \sigma_r(m) = r \cdot m \) for all \( m \in M \).

Show that \( \sigma_r \in \text{End}(M) \) for all \( r \in R \) and \( \pi : R \to \text{End}(M) \) defined by \( \pi(r) = \sigma_r \) for all \( r \in R \) is a homomorphism of rings with unity.

**Solution:** Let \( r \in R \). For \( m, n \in M \) the calculation \( \sigma_r(m + n) = r \cdot (m + n) = r \cdot m + r \cdot n = \sigma_r(m) + \sigma_r(n) \) shows that \( \sigma_r : M \to M \) is an endomorphism of (additive) groups.
Let \( r, r' \in R \). We have just shown that \( \pi(r) = \sigma_r \in \text{End}(M) \). Note that \( \pi(r)(m) = \sigma_r(m) = r \cdot m \) for all \( m \in M \). Since
\[
\pi(r + r')(m) = (r + r') \cdot m = r \cdot m + r' \cdot m = \pi(r)(m) + \pi(r')(m) = (\pi(r) + \pi(r'))(m)
\]
for all \( m \in M \) it follows that \( \pi(r + r') = \pi(r) + \pi(r') \). Likewise
\[
\pi(rr')(m) = (rr') \cdot m = r \cdot (r' \cdot m) = \pi(r)(\pi(r')(m)) = (\pi(r) \circ \pi(r'))(m)
\]
for all \( m \in M \) shows that \( \pi(rr') = \pi(r) \circ \pi(r') \). Thus \( \pi \) is a ring homomorphism. Since \( \pi(1)(m) = 1 \cdot m = m = I_M(m) \) for all \( m \in M \) we have \( \pi(1) = I_M \). Therefore \( \pi \) is a homomorphism of rings with unity.

2. \textbf{(20 total)} Let \( M \) be a left \( R \)-module. For a non-empty subset \( S \) of \( M \) the subset of \( R \) defined by
\[
\text{ann}_R(S) = \{ r \in R \mid r \cdot s = 0 \ \forall s \in S \}
\]
is called the \textit{annihilator} of \( S \). If \( S = \{s\} \) is a singleton we write \( \text{ann}_R(s) \) for \( \text{ann}_R(\{s\}) \).

(a) \textbf{(8)} Suppose that \( N \) is a submodule of \( M \). Show that \( \text{ann}_R(N) \) is an ideal of \( R \).

\textbf{Solution}: Let \( I = \text{ann}_R(N) \). Then \( 0 \in I \) since \( 0 \cdot m = 0 \) for all \( m \in N \). Thus \( I \neq \emptyset \). Suppose \( r, r' \in I \) and \( n \in N \). Then \( (r-r') \cdot n = r \cdot n - r' \cdot n = 0 - 0 = 0 \) since \( n, -n \in N \). Thus \( r - r' \in I \) which establishes that \( I \) is an additive subgroup of \( R \). For \( r'' \in R \) the calculations
\[
(r''r) \cdot n = r'' \cdot (r \cdot n) = r'' \cdot 0 = 0
\]
and
\[
(rr'') \cdot n = r \cdot (r'' \cdot n) \in r \cdot N = (0)
\]
show that \( r''r, rr'' \in I \). Therefore \( I \) is an ideal of \( R \).
Now suppose \( m \in M \) is fixed.

(b) \((6)\) Show that \( \text{ann}_R(m) \) is a left ideal of \( R \).

**Solution:** The calculations of part (a) establish part (b).

(c) \((6)\) Let \( f : R \longrightarrow R \cdot m \) be defined by \( f(r) = r \cdot m \) for all \( r \in R \). Show \( f \) is a homomorphism of left \( R \)-modules and \( F : R/\text{ann}_R(m) \longrightarrow R \cdot m \) given by \( F(r + \text{ann}_R(m)) = r \cdot m \) for all \( r \in R \) is a well-defined isomorphism of left \( R \)-modules.

**Solution:** Let \( r, r' \in R \). Then \( R \cdot m \) is a submodule of \( M \) (a proof really is in order) and the calculations

\[
f(r + r') = (r + r') \cdot m = r \cdot m + r' \cdot m = f(r) + f(r')
\]

and

\[
f(rr') = (rr') \cdot m = r \cdot (r' \cdot m) = r \cdot f(r')
\]

show that \( f \) is a map of left \( R \)-modules. One could appeal to the Isomorphism Theorems for \( R \)-modules to complete the problem; we will follow the intent of the instructions.

\( F \) is well-defined. Suppose that \( r, r' \in R \) and \( r + \text{ann}_R(m) = r' + \text{ann}_R(m) \). Then \( r - r' \in \text{ann}_R(m) \) which means \( (r - r') \cdot m = 0 \) or equivalently \( r \cdot m = r' \cdot m \). Therefore \( F(r + \text{ann}_R(m)) = r \cdot m = r' \cdot m = F(r' + \text{ann}_R(m)) \) which means \( F \) is well-defined. Note that \( F \) and \( f \) are related by \( F(r + \text{ann}_R(m)) = f(r) \) for all \( r \in R \).

\( F \) is a module map since

\[
F((r + \text{ann}_R(m)) + (r' + \text{ann}_R(m)))
= F((r + r') + \text{ann}_R(m))
= f(r + r')
= f(r) + f(r')
= F(r + \text{ann}_R(m)) + F(r' + \text{ann}_R(m))
\]

and

\[
F(r \cdot (r' + \text{ann}_R(m)))
\]
\[ F(r'r' + \text{ann}_R(m)) = f(r'r') = r'F(r' + \text{ann}_R(m)) \]

for all \( r, r' \in R \). \( F \) is surjective since \( f \) is. Since \( \ker F = \{ r + \text{ann}_R(m) \mid r \in \text{ann}_R(m) \} \) is the trivial subgroup of \( R/\text{ann}_R(m) \), it follows that the (group) homomorphism \( F \) is injective.

3. (20 total) Let \( k \) be a field, \( V \) a vector space over \( k \), and \( T \in \text{End}_k(V) \) be a linear endomorphism of \( V \). Then the ring homomorphism \( \pi : k[X] \rightarrow \text{End}_k(V) \) defined by \( \pi(f(X)) = f(T) \) for all \( f(X) \in k[X] \) determines a left \( k[X] \)-module structure on \( V \) by \( f(X) \cdot v = \pi(f(X))(v) = p(T)(v) \) for all \( v \in V \).

(a) (15) Let \( W \) be a non-empty subset of \( V \). Show that \( W \) is a \( k[X] \)-submodule of \( V \) if and only if \( W \) is a \( T \)-invariant subspace of \( V \).

Solution: Suppose that \( f(X) = \alpha_0 + \cdots + \alpha_nX^n \in k[X] \). Then \( f(X) \cdot v = f(T)(v) = (\alpha_0 I_V + \cdots + \alpha_n T^n)(v) = \alpha_0 v + \cdots + \alpha_n T^n(v) \) for all \( v \in V \). Let \( W \) be a \( k[X] \)-submodule. Then \( W \) is an additive subgroup of \( V \) by definition. Let \( w \in W \). Since \( f(X) \cdot w = \alpha_0 w \) when \( f(X) = \alpha_0 \) and \( f(X) \cdot w = T(w) \) when \( f(X) = X \), \( \alpha_0 w \in W \) for all \( \alpha_0 \in k \), which means that \( W \) is a subspace of \( V \), and \( T(w) \in W \), which means that \( W \) is \( T \)-invariant (or \( T \)-stable).

Conversely, let \( W \) be a \( T \)-invariant subspace of \( V \). Then \( T^m(W) \subseteq W \) for all \( m \geq 0 \) by induction on \( m \). Therefore \( f(X) \cdot w \in W \) for all \( w \in W \) which means that \( W \) is a \( k[X] \)-submodule of \( V \).

(b) (5) Suppose that \( V = k[X] \cdot v \) is a cyclic \( k[X] \)-module. Show that \( \text{ann}_{k[X]}(V) = (f(X)) \), where \( f(X) \) is the minimal polynomial of \( T \).

Solution: There are various ways of defining the minimal polynomial of \( T \). One is the unique monic generator of the ideal \( I \) of all
\( f(X) \in k[X] \) such that \( f(T) = 0 \) when \( I \neq (0) \). Otherwise the minimal polynomial is set to 0 when \( I = (0) \). Note that \( I = \text{ann}_{k[X]}(V) \).

Comment: The condition \( V \) is cyclic is not necessary; it was there anticipating a certain application.

4. (20 total) Let \( M \) be a left \( R \)-module.

(a) (5) Suppose that \( \mathcal{N} \) is a non-empty family of submodules of \( M \). Show that \( L = \bigcap_{N \in \mathcal{N}} N \) is a submodule of \( M \).

Solution: Since submodules are (additive) subgroups, we know from group theory that \( L = \bigcap_{N \in \mathcal{N}} N \) is a subgroup of \( M \). Let \( r \in R \) and \( n \in L \). To complete the proof that \( L \) is a submodule of \( M \) we need only show that \( r \cdot n \in L \). Since \( n \in L \), \( n \in N \) for all \( N \in \mathcal{N} \). Hence \( r \cdot n \in N \) for all \( N \in \mathcal{N} \), since each \( N \) is a submodule of \( M \), and therefore \( r \cdot n \in L \).

Since \( M \) is submodule of \( M \), it follows that any \( S \) subset of \( M \) is contained in a smallest submodule of \( M \), namely the intersection of all submodule containing \( S \). This submodule is denoted by \( (S) \) and is called the submodule of \( M \) generated by \( S \).

(b) (5) Let \( \emptyset \neq S \subseteq M \). Show that

\[ (S) = \{r_1 \cdot s_1 + \cdots + r_{\ell} \cdot s_{\ell} \mid \ell \geq 1, r_1, \ldots, r_{\ell} \in R, s_1, \ldots, s_{\ell} \in S\} \]

Solution: Let

\[ L' = \{r_1 \cdot s_1 + \cdots + r_{\ell} s_{\ell} \mid \ell \geq 1, r_1, \ldots, r_{\ell} \in R, s_1, \ldots, s_{\ell} \in S\} \]

Informally we may describe \( L' \) as the set of all finite sums of products \( r \cdot s \), where \( r \in R \) and \( s \in S \). Now \( L' \subseteq (S) \). For since \( S \subseteq (S) \) and \( (S) \) is a submodule of \( M \), products \( r \cdot s \in (S) \) since \( (S) \) is closed under module multiplication, and thus \( r_1 \cdot s_1 + \cdots + r_{\ell} s_{\ell} \in (S) \), by induction on \( \ell \), for all \( r_1, \ldots, r_{\ell} \in R \) and \( s_1, \ldots, s_{\ell} \in S \) since \( (S) \) is closed under addition.
To complete the proof we need only show \((S) \subseteq L'\). Since \(s = 1 \cdot s\) for all \(s \in M\) it follows that \(S \subseteq L'\). Thus to show \((S) \subseteq L'\) we need only show that \(L'\) is a submodule of \(M\). Since \(S \neq \emptyset\) and \(S \subseteq L'\) it follows that \(L' \neq \emptyset\).

Suppose that \(x, y \in L'\). Then \(x, y\) are finite sums of products \(r \cdot s\), where \(r \in R\) and \(s \in S\); therefore \(x + y\) is as well. We have shown \(x + y \in L'\). Since \(- (r \cdot s) = (r') \cdot (r \cdot s)\) for \(r, r' \in R\) and \(s \in S\), it follows that \(-x\) and \(r' \cdot x\) are finite sums of products \(r'' \cdot s''\), where \(r'' \in R\) and \(s'' \in S\). Therefore \(-x, r \cdot x \in L'\) which completes our proof that \(L'\) is a submodule of \(M\).

\textit{Comment:} Here are the highlights of a proof of the fact the \(L'\) is a submodule of \(M\) which follows the literal description of \(L'\).

Let \(x, y \in L'\). Write \(x = r_1 \cdot s_1 + \cdots + r_\ell \cdot s_\ell\) and \(y = r'_1 \cdot s'_1 + \cdots + r'_{\ell'} \cdot s'_{\ell'}\), where \(\ell, \ell' \geq 1\), \(r_1, \ldots, r_\ell, r'_1, \ldots, r'_{\ell'} \in R\), and \(s_1, \ldots, s_\ell, s'_1, \ldots, s'_{\ell'} \in S\). Thus

\[x + y = r_1 \cdot s_1 + \cdots + r_\ell \cdot s_\ell + r'_1 \cdot s'_1 + \cdots + r'_{\ell'} \cdot s'_{\ell'}\]

which means

\[x + y = r''_1 \cdot s''_1 + \cdots + r''_{\ell''} \cdot s''_{\ell''}\]

where \(\ell'' = \ell + \ell'\),

\[r''_i = \begin{cases} r_i & : 1 \leq i \leq \ell \\ r'_{i - \ell} & : \ell < i \leq \ell + \ell' \end{cases}\]

and

\[s''_i = \begin{cases} s_i & : 1 \leq i \leq \ell \\ s'_{i - \ell} & : \ell < i \leq \ell + \ell' \end{cases}\]

Thus \(x + y \in L'\). Note that

\[-x = -(r_1 \cdot s_1) - \cdots - (r_\ell \cdot s_\ell) = (-r_1) \cdot s_1 + \cdots + (-r_\ell) \cdot s_\ell \in L'\]

and

\[r \cdot x = r \cdot (r_1 \cdot s_1) + \cdots + r \cdot (r_\ell \cdot s_\ell) = (rr_1) \cdot s_1 + \cdots + (rr_\ell) \cdot s_\ell \in L'.\]

Suppose \(f, f' : M \rightarrow M'\) are \(R\)-module homomorphisms.
(c) (5) Show that \( N = \{m \in M \mid f(m) = f'(m)\} \) is a submodule of \( M \).

**Solution:** First of all \( 0 \in N \) since \( f(0) = 0 = f'(0) \) as \( f, f' \) are group homomorphisms. Suppose that \( m, n \in M \). Then \( f(m - n) = f(m + (-n)) = f(m) + f(-n) = f(m) - f(n) \). Thus for \( m, n \in N \) we have

\[
f(m - n) = f(m) - f(n) = f'(m) - f'(n) = f'(m - n)
\]

which means \( m - n \in N \). Therefore \( N \leq M \). For \( r \in R \) the calculation

\[
f(r \cdot m) = r \cdot f(m) = r \cdot f'(m) = f'(r \cdot m)
\]

shows that \( r \cdot m \in N \). Therefore \( N \) is a submodule of \( M \).

(d) (5) Suppose that \( S \) generates \( M \). Show that \( f = f' \) if and only if \( f(s) = f'(s) \) for all \( s \in S \).

**Solution:** If \( f = f' \) then \( f(s) = f'(s) \) for all \( s \in M \), hence for all \( s \in S \). Conversely, suppose that \( f(s) = f'(s) \) for all \( s \in S \) and let \( N \) be as in part (a). Then \( S \subseteq N \) which means \( M = (S) \subseteq N \) since \( S \) generates \( M \) and \( N \) is a submodule of \( M \). Therefore \( M = N \) which means \( f(m) = f'(m) \) for all \( m \in M \), or equivalently \( f = f' \).

**Comment:** There is no need to invoke part (b) for part (d).

5. **(20 total)** Use Corollary 2 of “Section 2.3 Supplement” and the equation of Problem 3 of Written Homework 3 to prove the following:

**Theorem 1** Let \( k \) be a field and suppose that \( G \) is a finite subgroup of \( k^\times \). Then \( G \) is cyclic.

**Solution:** A proof is to be based on the equations

\[
\sum_{d|n} \varphi(d) = n
\]

for all positive integers \( n \) and

\[
\sum_{d | |G|} n_d \varphi(d) = |G|
\]
for all finite groups $G$. Suppose that $H \leq k^\times$ is cyclic of order $d$. Then $a^d = 1$, or equivalently $a$ is a root of $X^d - 1 \in k[X]$, for all $a \in H$. This polynomial has at most $d$ roots in $k$ since $k$ is a field. Therefore $H$ is the set of the roots of $X^d - 1$ in $k$. We have shown that there is at most one cyclic subgroup of order $d$ in $k^\times$.

Now let $G \leq k^\times$ be finite. We have shown $n_d = 0$ or $n_d = 1$ for each positive divisor of $|G|$. Since $\varphi(d) > 0$ for all positive integers $d$, from the equations

$$\sum_{d \mid |G|} n_d \varphi(d) = |G| = \sum_{d \mid |G|} \varphi(d) = \sum_{d \mid |G|} 1 \varphi(d)$$

we deduce that $n_d = 1$ for all positive divisors $d$ of $|G|$. In particular $n_{|G|} = 1$ which means that $G$ has a cyclic subgroup of order $|G|$; thus $G$ is cyclic.