Problem 1 (12.1). *1. Let R be a ring and M and R-module. Prove that $r0 = 0$ for $r \in R$. If R has the identity 1, then $(-1)x = -x$ for $x \in M$.*

2. Let R be a ring and M, N, L be R-modules. Prove:

(a) $\hom_R(M, N)$ *is an abelian group under addition*

$$(\phi + \psi)(m) = \phi(m) + \psi(m)$$

If R is commutative, $\hom(M, N)$ *is an R-module with the R-action given by*

$$(r\phi)(m) = r\phi(m)$$

(b) If $\phi \in \hom_R(M, N)$ and $\psi \in \hom_R(N, L)$, then $\psi \circ \phi \in \hom_R(M, L)$.

(c) $\hom_R(M, M)$ *is a ring with identity with composition as multiplication.*

3. Prove that $\hom_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_m) \cong \mathbb{Z}_d$ *where* $d = \gcd(m, n)$.

Proof. 1. Note that $r0 = r(0 + 0) = r0 + r0$. Subtract an $r0$ from each side and you get that $0 = r0$ for all $r \in R$.

For the second part. We have that

$$0 = 0x = (1 - 1)x = 1x + (-1)x = x + (-1)x$$

which implies that $(-1)x = -x$.

2. (a) The group operation will be associative because it is adding group elements and the addition of group elements is associative. The identity will be the function $z(m) = 0$ as

$$(\phi + z)(m) = \phi(m) + 0 = \phi(m)$$

The inverse for $\phi \in \hom(M, N)$ will be $\psi(m) = -\phi(m)$ as

$$(\phi + \psi)(m) = \phi(m) - \phi(m) = 0$$

Since we have all of the group axioms fulfilled $\hom_R(M, N)$ is a group.
To show that $\hom_R(M, N)$ is an R-module when R is commutative we will verify the four axioms from the notes. We will have $r, s \in R$ with $\phi, \psi \in \hom_R(M, N)$, and $m \in M$ further down.

i. Start with $(r + s)\phi$. Then for an arbitrary element m we have

$$(r + s)\phi(m) = r\phi(m) + s\phi(m)$$

from the fact that N is an R-module.

ii. For the next we have

$$(rs)\phi(m) = r(s\phi(m))$$

which shows that

$$(rs)\phi = r(s\phi)$$

following from N being an R module.

iii. Next we have

$$r(\phi + \psi)(m) = r(\phi(m) + \psi(m)) = r\phi(m) + r\psi(m)$$

following from N being an R module which shows that

$$r(\phi + \psi) = r\phi + r\psi$$

iv. Finally

$$1\phi(m) = \phi(m)$$

as N is an R-module which implies that

$$1\phi = \phi$$

This completes the proof.

(b) We know that $\psi \circ \phi \in \hom(M, L)$ because they are group homomorphisms. As such all we have to show is that the composition preserves the R-module structure. Let $r \in R$. Then from the fact that ϕ, ψ are R-module homomorphisms we have that

$$\psi \circ \phi(rm) = \psi(r\phi(m)) = r\psi \circ \phi(m)$$

which verifies that $\psi \circ \phi$ is a homomorphism of R-modules and as such $\psi \circ \phi \in \hom_R(M, L)$.

(c) We know from above that $\hom_R(M, M)$ is a group under addition of maps, that the composition is well defined, and that composition is associative with identity (id_M) in general. Thus the only remaining portion to show is that composition distributes over addition of maps. Let $\phi, \psi, \varphi \in \hom_R(M, N)$. Then

$$\varphi \circ (\phi + \psi)(m) = \varphi(\phi(m) + \psi(m)) = \varphi \circ \phi(m) + \varphi \circ \psi(m)$$

Thus composition distributes over addition of maps and therefore $\hom_R(M, M)$ forms a ring.

3. From a previous assignment we know that all homomorphisms in $\hom_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_m)$ are of the form $\phi_k(x) = kx$. The maps ϕ_k will be in $\hom_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_m)$ only when $nk \equiv 0 \mod m$ ($nk = mq$ for some $q \in \mathbb{Z}$). The number of ks that fulfill this requirement is $\gcd(m, n) = d$. Then consider the map ϕ_a where $a = \frac{m}{d}$. If we add ϕ_a to itself we will get $\frac{m}{a} = d$ different homomorphisms before reaching the identity. Since the group $\hom_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_m)$ has d elements and is cyclic it must be isomorphic to $\mathbb{Z}_d$.

$\square$

Problem 2 (12.2)**.** *Let A, B be submodules of an R-module M. Prove that $A + B$ and $A \cap B$ are submodules of M. Moreover, the equality*

$$A \cap (B + C) = B + (A \cap C)$$

holds for all R-submodules C if $B \subseteq A$.

Proof. As A, B are submodules of M they are also subgroups and as such $A + B, A \cap B$ are closed under the group operations. The only thing left to verify is that they are closed under the action of R.

Let $r \in R$ and $a + b \in A + B$ with $a \in A$ and $b \in B$. Then $r(a + b) = ra + rb$ and since $ra \in A$ and $rb \in B$ we have that $r(a + b) = ra + rb \in A + B$. Therefore $A + B$ is a submodule.

Next let $m \in A \cap B$. Then $rm \in A$ and $rm \in B$ which implies that $rm \in A \cap B$. Therefore $A \cap B$ is a submodule.

Now suppose that $B \subseteq A$ where A, B, C are submodules of M. Let $m \in A \cap (B + C)$. Then $m = b + c$ where $b \in B$ and $c \in C$ and $b + c \in A$. However since $b \in A$, as $B \subseteq A$, we have that $c = (b + c) - b \in A$. Therefore $m = b + c \in B + (A \cap C)$ and thus $A \cap (B + C) \subseteq B + (A \cap C)$.

Let $m \in B + (A \cap C)$. Then $m = b + c$ where $b \in B$ and $c \in A \cap C$. However since $B \subseteq A$ we have that $b \in A$ which implies that $b + c \in A$ and that $b + c \in B + C$. Thus $m \in A \cap (B + C)$ and therefore $B + (A \cap C) \subseteq A \cap (B + C)$.

Therefore if $B \subseteq A$ then $A \cap (B + C) = B + (A \cap C)$. $\square$

Problem 3 (12.4)**.** *Let M be an R-module.*

1. *For any submodules $N_1, \dots, N_n$ of M, their sum $N_1 + \cdots + N_n$ is the smallest submodule of M which contains $N_1 \cup \cdots \cup N_n$.*

2. *For any subset A of M, RA is the smallest submodule of M which contains A.*

Proof. 1. Since we are summing a finite number of submodules the fact that $N_1 + \cdots + N_n$ is a submodule follows from the previous problem. Let N be a submodule of M such that $\bigcup_i N_i \subseteq N$ and let $\sum_i k_i \in N_1 + \cdots + N_n$ with $k_i \in N_i$. Then $k_i \in N$ for all i. However since submodules are closed under addition we have that $\sum_i k_i \in N$. As this holds for an arbitrary element of $N_1 + \cdots + N_n$ it must be that $N_1 + \cdots + N_n \subseteq N$.

   Therefore if N is a submodule such that $\bigcup_i N_i \subseteq N$ then $N_1 + \cdots + N_n \subseteq N$.

2. We know that RA will be a submodule from the notes. Let N be a submodule of M such that $A \subset N$ and let $ra \in RA$. Since $a \in N$ and N is a submodule then $ra \in N$ which implies that $RA \subset N$.

   Therefore if $A \subseteq M$ then any submodule N that contains A will contain RA.

$\square$

Problem 4 (12.5)**.** *Show that $\mathbb{Z}_{p^e}$, regarded as a $\mathbb{Z}$-module is not a direct sum of any two non-zero submodules, where p is a prime and $e > 0$. Does it hold for $\mathbb{Z}$? Does it hold for $\mathbb{Z}_{12}$?*

Proof. Suppose that $\mathbb{Z}_{p^e} \cong \mathbb{Z}_{p^a} \oplus \mathbb{Z}_{p^b}$ where $b, a > 0$. The decomposition would have to be of this form because of the orders. However this is the same as implies that $\mathbb{Z}_{p^e} \cong \mathbb{Z}_{p^a} \times \mathbb{Z}_{p^b}$. However the group on the right is not cyclic which is a contradiction. $\square$

This does not hold for $\mathbb{Z}_{12}$ as $\mathbb{Z}_{12} \cong \langle 3 \rangle + \langle 4 \rangle$.

This does hold for $\mathbb{Z}$ as any submodules will be isomorphic to $\mathbb{Z}$ and as such the direct sum would be $\mathbb{Z} \oplus \mathbb{Z}$ which is not isomorphic to $\mathbb{Z}$.

Problem 5 (12.7)**.** *Let R be a PID and p a prime in R.*

1. *If M is a finitely generated p-primary R-module, then M/pM is an $R/(p)$-module with the R-action given by*
$$(r + (p))(x + pM) := rx + pM$$
   Moreover, show that the mapping ϕ defined in
$$\phi(r_1 x_1 + \cdots + r_m x_m + pM) = (\bar{r}_1, \dots, \bar{r}_m)$$
   is a $R/(p)$-module map.

2. *Let $\phi : M_1 \to M_2$ be an isomorphism finitely generated p-primary R-modules. Prove that $\phi|_{pM_1} : pM_1 \to pM_2$ is an isomorphism of R-module. Show that the map $\bar{\phi} : M_1/pM_1 \to M_2/pM_2$ defined by*
$$\bar{\phi}(m + pM_1) = \phi(m) + pM_2$$
   is an isomorphism of $R/(p)$-vector spaces.

Proof. 1. M/pM is already a quotient group and as such we do not need to verify the group axioms. From here on in this problem $r, s \in R$ and $x, y \in M$.

(a) Start with $((r+(p))+(s+(p)))(x+pM)$ to get

$$((r+(p))+(s+(p)))(x+pM) = ((r+s)+(p))(x+pM)$$
$$= (r+s)x + pM = rx + sx + pM = (rx+pM) + (sx+pM)$$
$$= (r+(p))(x+pM) + (s+(p))(x+pM)$$

(b) Start with $((r+(p))(s+(p)))(x+pM)$ to get

$$((r+(p))(s+(p)))(x+pM) = (rs + r(p) + s(p) + (p))(x+pM) =$$
$$(rs+(p))(x+pM) = (rs)x + pM = r(sx) + pM = (r+(p))(sx+pM)$$
$$(r+(p))((s+(p))(x+pM))$$

(c) Start with $(r+(p))((x+pM)+(y+pM))$ to get

$$(r+(p))((x+pM)+(y+pM)) = (r+(p))((x+y)+pM)$$
$$= r(x+y) + pM = (rx+ry) + pM = (rx+pM) + (ry+pM)$$
$$= (r+(p))(x+pM) + (r+(p))(y+pM)$$

(d) Finally begin with $(1+(p))(x+pM)$ to get

$$(1+(p))(x+pM) = 1x + pM = x + pM$$

.

Since all of the axioms for a module are fulfilled it is true that M/pM is an $R/(p)$-module with the action as defined above.

Now we will show that ϕ is an R-module map. This map is already a homomorphism of groups since the x_is form a basis. Thus all that is left to check is that the $R/(p)$ action plays nicely with the map $\bar{\phi}$. Let $r+(p) \in R/(p)$ and $\sum_1^m r_i x_i + pM \in M/pM$. Then

$$\phi((r+(p))(\sum_1^m r_i x_i + pM)) = \phi(\sum_1^m r r_i x_i) = (r\bar{r}_1, \ldots, r\bar{r}_m)$$

$$= ((r+(p))\bar{r_1}, \ldots, (r+(p))\bar{r_m}) = (r+(p))(\bar{r}_1, \ldots, \bar{r_m}) = (r+(p))\phi(\sum_1^m r_i x_i + pM)$$

which shows that ϕ is indeed an $R/(p)$ module map.

2. Since the map ϕ is injective we know that the restriction will be as well. Thus the only portion left to show is that $\phi(pM_1) = pM_2$. To show this let $m \in pM_2$. Then $p^l m = 0$ for some l. Since ϕ is an isomorphism we have $\phi(p^l)^{-1}\phi^{-1}(m) = 0$ which means that $\phi^{-1}(m) \in pM_1$ and as such $\phi(\phi^{-1}(m)) = m$. Therefore $\phi(pM_1) = pM_2$ and as such $\phi|_{pM_1}$ is an isomorphism.

   Since the map ϕ is an isomorphism and we are quotienting out by isomorphic submodules it then follows that $\bar{\phi}$ will be an isomorphism between M_1/pM_1 and M_2/pM_2 as it will respect the action of $R/(p)$.

□

Problem 6 (12.8). *1. Find the Smith normal form of the integer matrix*

$$\begin{bmatrix} 2 & 1 & 3 \\ 1 & -1 & 2 \end{bmatrix}$$

2. *Determine the invariant factor decomposition of $\mathbb{Z}^3/K$ where K is generated by $f_1(2,1,-3)$ and $f_2 = (1,-1,2)$.*

Proof. 1. The Smith normal form of the above matrix is

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} -3 & 2 & -5 \\ 0 & 0 & 1 \\ 2 & -1 & 3 \end{pmatrix}$$

2. The Smith normal form of the matrix with rows of f_1, f_2 is

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

Which means that the invariant factor decomposition will be $\mathbb{Z}$.

□

Problem 7 (12.9)**.** *1. Find a basis for the submodule K of $\mathbb{Q}[x]^3$ generated by*

$$f_1 = (2x-1, x, x^2+3), \quad f_2 = (x, x, x^2), \quad f_3 = (x+1, 2x, 2x^2-3)$$

2. Find the invariant factors and elementary divisors of the $\mathbb{Q}[x]$-module $\mathbb{Q}[x]^3/K$.

Proof. 1. The Smith normal form of the matrix with f_is as rows will be

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

Thus the basis will be $(1, x)$

2. The invariant factor will be x. The elementary divisor is x.

□

Problem 8 (12.11)**.** *Let F be a field and V an n-dimensional vector space over F with an ordered basis $\mathcal{B}$.*

1. *Let T be a linear operator on V. For any ordered basis $\mathcal{B}'$ of V, the matrices $[T]_{\mathcal{B}}$ and $[T]_{\mathcal{B}'}$ are similar over F. Conversely, if $A \in M_n(F)$ is similar to $[T]_{\mathcal{B}}$ over F, there exists a basis $\mathcal{B}'$ such that $[T]_{\mathcal{B}'} = A$.*

2. *Two F-linear operators S, T on V are similar if, and only if, the matrices $[T]_{\mathcal{B}}$ and $[S]_{\mathcal{B}}$ are similar.*

Proof. 1. Let $\mathcal{B}$ and $\mathcal{B}'$ be ordered bases. Then there is an invertible matrix P that changes from one basis to the other ($\mathcal{B} = P\mathcal{B}'$). Then

$$[T]_{\mathcal{B}} = [T]_{P\mathcal{B}'} = P[T]_{\mathcal{B}'}P^{-1}$$

which shows that they are similar.

Now let $A \in M_n(F)$ and $A \sim [T]_{\mathcal{B}}$ over F. Then $A = P[T]_{\mathcal{B}}P^{-1}$ for an invertible matrix P. Let $\mathcal{B}' = P\mathcal{B}$. Then $[T]_{\mathcal{B}'} = A$ because of the prior part of this part.

2. Let S, T be similar linear transformations. Then there is an isomorphism of vector spaces $\varphi : V \to V$ such that $S = \varphi \circ T \circ \varphi^{-1}$. However given an ordered basis $\mathcal{B}$ we can express the prior equation as

$$[S]_{\mathcal{B}} = [\varphi]_{\mathcal{B}}[T]_{\mathcal{B}}[\varphi^{-1}]_{\mathcal{B}}$$

which shows that $[S]_{\mathcal{B}} \sim [T]_{\mathcal{B}}$.

Now suppose that $[S]_{\mathcal{B}} \sim [T]_{\mathcal{B}}$. Then there is an invertible matrix P such that $[S]_{\mathcal{B}} = P[T]_{\mathcal{B}}P^{-1}$ which shows that the matrix P corresponds to an isomorphism. It then follows that S and T are similar.

Therefore two F-linear operators are similar if and only if their matrices with respect to an ordered basis are similar.

$\square$

Problem 9 (12.13)**.** *Find the rational canonical form of the matrix*

$$A = \begin{bmatrix} -1 & -2 & 6 \\ -1 & 0 & 3 \\ -1 & -1 & 4 \end{bmatrix} \in M_3(\mathbb{Q})$$

Consider $A \in M_3(\mathbb{C})$ and find the Jordan canonical form of A.

To find the canonical form we start with

$$xI - A = \begin{pmatrix} 1+x & 2 & -6 \\ 1 & x & -3 \\ 1 & 1 & x-4 \end{pmatrix}$$

which we then reduce to

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & x-1 & 0 \\ 0 & 0 & -x^2+2x-1 \end{pmatrix}$$

Which gives us the rational canonical form

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 2 \end{pmatrix}$$

and the Jordan canonical from

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