# INTRODUCTION TO CATEGORY THEORY

ROBERT CARDONA, MASSY KHOSHBIN, AND SIAVASH MORTEZAVI

Abstract. Category Theory: Remain calm and carry on when all the mathematics you've ever known and loved gets abstracted away into dots and arrows.

## 0. MATH 697 Homework Zero

**Exercise.** (DF §10.2 Theorem 4): Prove Theorem 4 (Isomorphism Theorems):

(1) (*The First Isomorphism Theorem for Modules*) Let $M, N$ be $R$-modules and let $\varphi : M \to N$ be an $R$-modules homomorphism. Then $\ker\varphi$ is a submodule of $M$ and $M/\ker\varphi \cong \varphi(M)$.

*Proof.* Let $M, N$ be $R$-modules and let $\varphi : M \to N$ be an $R$-modules homomorphism. Then by definition $\varphi(x+y) = \varphi(x) + \varphi(y)$ and $\varphi(rx) = r\varphi(x)$ for all $x, y \in M$, $r \in R$. We want to show that $\ker\varphi = \{m \in M : \varphi(m) = 0\}$ is a submodule. Observe that since $M$ is a module then $M$ is an abelian group by definition so there exists $0 \in M$ such that $m+0 = m$ for all $m \in M$. In particular $\varphi(0) = \varphi(0+0) = \varphi(0)+\varphi(0)$ implying $\varphi(0) = 0$. Conclude that $0 \in \ker\varphi \neq \emptyset$. Now let $r \in R$, $x, y \in \ker\varphi$. Observe that $\varphi(x+ry) = \varphi(x) + \varphi(ry) = \varphi(x) + r\varphi(y) = 0 + r \cdot 0 = 0 + 0 = 0$. Hence $x + ry \in \ker\varphi$. Conclude by the submodule criterion that $\ker\varphi$ is in fact a submodule.

Now define $\Phi : M/\ker\varphi \to \varphi(M)$ by $\Phi(m + \ker\varphi) = \varphi(m)$. We want to show that this mapping is a well-defined bijective homomorphism. We first show well-definedness. Suppose $m + \ker\varphi = m' + \ker\varphi$ it follows by property of cosets that $m - m' \in \ker\varphi$, in particular $\varphi(m - m') = \varphi(m) - \varphi(m') = 0$ and hence $\varphi(m) = \varphi(m')$. But since $\varphi(m) = \Phi(m + \ker\varphi)$ and $\varphi(m') = \Phi(m' + \ker\varphi)$ we have $\Phi(m + \ker\varphi) = \Phi(m' + \ker\varphi)$. Conclude that $\Phi$ is in fact well-defined.

Suppose that $\Phi(m + \ker\varphi) = \Phi(m' + \ker\varphi)$. Then it follows that $\varphi(m) = \varphi(m')$ and so $\varphi(m - m') = 0$ and so $m - m' \in \ker\varphi$. By property of cosets it follows that $m + \ker\varphi = m' + \ker\varphi$ and hence $\Phi$ is injective.

Let $n \in \varphi(M)$. Then by definition of image of $\varphi$ there exists $m \in M$ such that $n = \varphi(m)$. It is immediate that $m + \ker\varphi \in M/\ker\varphi$ and we can conclude that $\Phi$ is surjective.

Now we must show that $\Phi$ is an $R$-module homomorphism. Let $x, y \in M/\ker\varphi$ where $x = m + \ker\varphi$ and $y = m' + \ker\varphi$ for some $m, m' \in M$ and let $r \in R$. Observe that

$$\begin{aligned}
\Phi(x+y) &= \Phi(m + m' + \ker\varphi) \\
&= \varphi(m + m') \\
&= \varphi(m) + \varphi(m') \\
&= \Phi(m + \ker\varphi) + \Phi(m' + \ker\varphi) \\
&= \Phi(x) + \Phi(y)
\end{aligned}$$

and

$$\begin{aligned}
\Phi(rx) &= \Phi(r(m + \ker\varphi)) \\
&= \Phi(rm + \ker\varphi) \\
&= \varphi(rm) \\
&= r\varphi(m) \\
&= r\Phi(m + \ker\varphi) \\
&= r\Phi(x)
\end{aligned}$$

Hence we have shown that $\Phi$ is a well-defined bijective homomorphism and thus we can conclude by definition of $R$-module isomorphism that $M/\ker\varphi \cong \varphi(M)$. □

(2) (*The Second Isomorphism Theorem*) Let $A, B$ be submodules of the $R$-module $M$. Then $(A + B)/B \cong A/(A \cap B)$.

*Date*: July 8, 2013.

*Proof.* Define $\varphi : A \to (A+B)/B$ by $\varphi(a) = a + B$. This mapping is clearly well-defined. We want to show that $\varphi$ is a homomorphism. Let $r \in R$, $a, a' \in A$ and observe that

$$\begin{aligned} \varphi(a+a') &= a + a' + B \\ &= a + B + a' + B \\ &= \varphi(a) + \varphi(a') \end{aligned}$$

and

$$\begin{aligned} \varphi(ra) &= ra + B \\ &= r(a+B) \\ &= r\varphi(a) \end{aligned}$$

and so $\varphi$ is an $R$-module homomorphism by definition. Observe that $\ker\varphi = \{a \in A : \varphi(a) = 0\} = \{a \in A : a + B = 0\} = \{a \in A : a \in B\} = A \cap B$. Now let $x \in (A+B)/B$ then $x = a + b + B$ for some $a \in A$, $b \in B$. But observe that $a+b+B = a+B$ by absorbption. So $\varphi$ is immediately surjective. In particular we have $\varphi(A) = (A+B)/B$. Conclude by the First Isomorphism Theorem for Modules that $A/\ker\varphi = A/(A\cap B) \cong (A+B)/B = \varphi(A)$. □

(3) (*The Third Isomorphism Theorem*) Let $M$ be an $R$-module, and let $A$ and $B$ be submodules of $M$ with $A \subseteq B$. Then $(M/A)/(B/A) \cong M/B$.

*Proof.* Define $\varphi M/A \to M/B$ by $\varphi(m+A) = m + B$. We need to show $\varphi$ is well-defined. Suppose $m + A = m' + A$ then $m - m' \in A \subseteq B$ by property of cosets. It also follows that $m + B = m' + B$. Hence $\varphi(m+A) = m + B = m' + B = \varphi(m' + A)$ and hence $\varphi$ is well-defined.

Now we must show $\varphi$ is an $R$-module homomorphism. Let $m, m' \in M$ and $r \in R$. Observe that

$$\begin{aligned} \varphi((m+A) + (m'+a)) &= \varphi(m + m' + A) \\ &= m + m' + B \\ &= (m+B) + (m'+B) \\ &= \varphi(m+A) + \varphi(m'+A) \end{aligned}$$

and

$$\begin{aligned} \varphi(r(m+A)) &= \varphi(rm + A) \\ &= rm + B \\ &= r(m+A) \\ &= r\varphi(m+A) \end{aligned}$$

and hence we can conclude by definition that $\varphi$ is an $R$-module homomorphism.

Observe that $\ker\varphi = \{x \in M/A : \varphi(x) = 0\} = \{m + A"\varphi(m+A) = m + B = 0\} = \{m + A : m \in B\} = B/A$. Let $m + B \in M/B$. Clearly $\varphi(m+A) = m + B$ and hence $\varphi$ is surjective. Now by the First Isomorphism Theorem for Modules we have $(M/A)/\ker\varphi = (M/A)/(B/A) \cong M/B = \varphi(M/A)$. □

(4) (*The Fourth or Lattice Isomorphism Theorem*) Let $N$ be a submodule of the $R$-module $M$. There is a bijection between the submodules of $M$ which contain $N$ and the submodules of $M/N$. The correspondence is given by $A \leftrightarrow A/N$, for all $A \supseteq N$. The correspondence cummutes with the processes of taking sums and intersections (i.e., is a lattice isomorphism between the lattice of submodules of $M/N$ and the lattice of submodules of $M$ which contain $N$).

*Proof.* Let $N$ be a submodule of $M$. Define $S = \{K : K \text{ is a submodule of } M, N \subseteq K\}$, $T = \{L : L \text{ is a submodule of } M/N\}$. Define $\varphi : S \to T$ by $\varphi(K) = K/N$. We want to show that this mapping is bijective.

Let $K_1, K_2 \in S$ and suppose that $\varphi(K_1) = \varphi(K_2)$. Then $K_1/N = K_2/N$. We want to show that $K_1 = K_2$. Let $x \in K_1$, then $x + N \in K_1/N = K_2/N$, in particular there exists $y \in K_2$ such that $x + N = y + N$. By property of cosets it follows that $x - y \in N$. But since $N \subseteq K_2$ by construction $x - y \in K_2$. Since $K_2$ is a submodule of $M$, it is closed under addition and so $(x-y) + y = x \in K_2$. Conclude that $K_1 \subseteq K_2$. By symmetric argument $K_2 \subseteq K_1$ and hence $K_1 = K_2$. Thus by definition $\varphi$ is injective.

Let $L$ be a submodule of $M/N$. Consider the natural projection map $\pi : M \to M/N$ defined by $\pi(m) = m + N$. We want to show that there exists $K \in S$ such that $\varphi(K) = L$. To do this we will show that $\pi^{-1}(L)$ is a submodule of $M$ and that $N \subseteq \pi^{-1}(L)$. Recall that $\pi^{-1}(L) = \{m \in M : \pi(m) \in L\}$. Observe that $0 \in \pi^{-1}(L)$ since $\pi(0) = 0$ and hence $\pi^{-1}(L) \neq \emptyset$. Let $x, y \in \pi^{-1}(L)$ and $r \in R$. Observe that $\pi(x + ry) = \pi(x) + r\pi(y)$. Since $\pi(y) \in L$ by definition and $L$ is a submodule of $M/N$, it follows that since scalar multiplication is closed $r\pi(y) \in L$. Thus it follows that $\pi(x) + r\pi(y) \in L$ and hence $x + ry \in \pi^{-1}(L)$. Thus by the submodule criterion we can conclude that $\pi^{-1}(L)$ is in fact a submodule. Now let $n \in N$ and observe that $\pi(n) = n + N = 0 + N \in L$ so by definition it follows that $n \in \pi^{-1}(L)$. Conclude that $N \subseteq \pi^{-1}(L)$ and hence $\varphi$ is surjective.

Conclude $\varphi$ is bijective and result follows. $\square$

**Exercise.** (DF §10.2 Exercise 1): Use the submodule criterion to show that the kernels and images of $R$-module homomorphisms are submodules.

*Proof.* Let $M, N$ be $R$-modules and $\varphi : M \to N$ an $R$-module homomorphism. Recall that $\ker\varphi = \{m \in M : \varphi(m) = 0\}$ and $\operatorname{im}\varphi = \{n \in N : \text{there exists } m \in M \text{ with } \varphi(m) = n\}$.

Observe that $\varphi(0) = 0$ so $0 \in \ker\varphi \neq \emptyset$. Let $m, m' \in M$, $r \in R$. Now $\varphi(m + rm') = \varphi(m) + r\varphi(m') = 0 + r \cdot 0 = 0 + 0 = 0$. So $m + rm' \in \ker\varphi$. Thus by the submodule criterion $\ker\varphi$ is a submodule.

Observe that $\varphi(0) = 0 \in N$ so $0 \in \operatorname{im}\varphi \neq \emptyset$. Let $n, n' \in N$, $r \in R$. Then there exists $m, m' \in M$ such that $\varphi(m) = n$ and $\varphi(m') = n'$. Now consider $n + rn'$. $\varphi(m + rm') = \varphi(m) + r\varphi(m') = n + rn'$ so $n + rn' \in \operatorname{im}\varphi$. Conclude by submodule criterion that $\operatorname{im}\varphi$ is in fact a submodule. $\square$

**Exercise.** (DF §10.2 Exercise 2): Show that the relation "is $R$-module isomorphic to" is an equivalence relation on any set of $R$-modules.

*Proof.* Let $X$ be a set of $R$-modules.

- Let $M \in X$. Observe that $M$ is isomorphic to $M$ trivially. So relation is reflexive.
- Let $M, N \in X$. Suppose $M$ is isomorphic to $N$ then by definition there exists $\varphi : M \to N$ that is bijective. Immediately we have $\varphi^{-1} : N \to M$ which is also bijective so $N$ is isomorphic to $M$. By definition the relation is symmetric.
- Let $L, M, N \in X$ . Suppose $L$ is isomorphic to $M$, then by definition there exists $\varphi : L \to M$ a bijective $R$-module homomorphism. Suppose $M$ is isomorphic to $N$, then there exists $\Phi : M \to N$ a bijective $R$-module homomorphism. Observe that $\varphi \circ \Phi : L \to N$ is again a bijective $R$-module homomorphism by property of composition of mappings. Hence by definition $L$ is isomorphic to $N$.

Conclude that the relation "is $R$-module isomorphic to" is an equivalence relation on any set of $R$-modules. $\square$

**Exercise.** (DF §10.2 Exercise 3): Give an explicit example of a map from one $R$-module to another which is a group homomorphism but not an $R$-module homomorphism.

*Solution.* Consider the Quaternions $\mathbb{H} = R$; they form a commutative group under addition and a noncommutative group under multiplication. Hence $\mathbb{H}$ is a noncommutative ring with unity. In particular $\mathbb{H}$ is an $R$-module over itself. Define $\varphi : \mathbb{H} \to \mathbb{H}$ by $\varphi(h) = ih$. This is a group homomorphism since $\varphi(h + h') = i(h + h') = ih + ih' = \varphi(h) + \varphi(h')$. But note that $\varphi(j \cdot 1) = \varphi(j) = ij = k \neq -k = ji = j(i \cdot 1) = j\varphi(1)$. Conclude that $\varphi$ is not an $R$-module homomorphism since the definition is not satisfied. ◀

**Exercise.** (DF §10.2 Exercise 4): Let $A$ be and $\mathbb{Z}$-module, let $a$ be any element of $A$ and let $n$ be a positive integer. Prove that the map $\varphi_a : \mathbb{Z}/n\mathbb{Z} \to A$ given by $\varphi(\overline{k}) = ka$ is a well-defined $\mathbb{Z}$-module homomorphism if and only if $na = 0$. Prove that $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A_n$, where $A_n = \{a \in A : na = 0\}$ (So $A_n$ is the annihilator in $A$ of the ideal $(n)$ of $\mathbb{Z}$).

*Proof.* Suppose that the map $\varphi_a : \mathbb{Z}/n\mathbb{Z} \to A$ given by $\varphi(\overline{k}) = ka$ is a well-defined $\mathbb{Z}$-module homomorphism. Then by definition if $\overline{m} = \overline{k}$ then $\varphi(\overline{m}) = \varphi(\overline{k})$ or equivalently $ma = ka$. Moreover $\varphi(a + b) = \varphi(a) + \varphi(b)$ and $\varphi(ra) = r\varphi(a)$ for all $a, b \in A$ and $r \in \mathbb{Z}$. Observe that $\overline{0} = \overline{k}$ so by hypothesis $\varphi(\overline{0}) = \varphi(\overline{k})$ but observe that $\varphi(\overline{0}) = 0 \cdot a = 0$ and $\varphi(\overline{k}) = ka$. Hence by equality $ka = 0$. Conversely suppose that $na = 0$. We want to show that $\varphi : \mathbb{Z}/n\mathbb{Z} \to A$ defined by $\varphi(\overline{k}) = ka$ is a well-defined $R$-module homomorphism. Say $\overline{k} = \overline{m}$ then by property of cosets $k - m \in \mathbb{Z}/n\mathbb{Z}$ and so $n \cong k - m$. By definition $n \mid k - m$ and hence there exists $t \in \mathbb{Z}$ such that $k - m = nt$. Observe that

$$\begin{aligned}
k - m &= nt \\
(k - m)a &= nta \\
ka - ma &= (na)t \\
ka - ma &= 0 \\
ka &= ma
\end{aligned}$$

Thus we have $\varphi(\overline{k}) = \varphi(\overline{m})$ and we can conclude that $\varphi$ is in fact a well-defined $R$-module homomorphism.

Now we want to show that $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A_n = \{a \in A : na = 0\}$. *Note*: We are making the assumption that we want to show this in an isomorphism of $R$-modules as exercise does not specifiy group, ring or module isomorphism. Define $\Phi : A_n \to \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A)$ by $\Phi(a) = \varphi_a$. We will show that this is in fact an $R$-module homomorphism, then that is a bijection.

Let $a, a' \in A_n$, $r \in \mathbb{Z}$. Observe that

$$\begin{aligned}
\Phi(a + a')(\overline{k}) &= \varphi_{a+a'}(\overline{k}) \\
&= (a + a')k \\
&= ak + a'k \\
&= \varphi_a(\overline{k}) + \varphi_{a'}(\overline{k})
\end{aligned}$$

$$= \Phi(a)(\overline{k}) + \Phi(a')(\overline{k})$$

So $\Phi(a+a') = \Phi(a) + \Phi(a')$ by definition. Moreover

$$\begin{aligned}\Phi(ra)(\overline{k}) &= \varphi_{ra}(\overline{k})\\ &= rak\\ &= r\varphi_a(\overline{k})\\ &= r\Phi(a)(\overline{k})\end{aligned}$$

Hence $\Phi(ra) = r\Phi(a)$ by definition. Conclude by definition that $\Phi$ is in fact an $R$-module homomorphism.

Recall that $\ker\Phi = \{a \in A_n : \Phi(a) = 0\}$ and observe that

$$\begin{aligned}\ker\varphi &= \{a \in A_n : \Phi(a) = 0\}\\ &= \{a \in A_n : \varphi_a(\overline{k}) = 0 \text{ for all k } \in \mathbb{Z}/n\mathbb{Z}\}\\ &= \{0\}\end{aligned}$$

So we conclude that $\ker\Phi = \{0\}$ and hence $\Phi$ is injective.

Let $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A_n)$. Define $a = \varphi(\overline{1})$ and hence $na = n\varphi(\overline{1}) = \varphi(n\overline{1}) = \varphi(\overline{n}) = \varphi(\overline{0}) = 0$ and hence $a \in A_n$. Observe that for all $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ it follows that $\varphi(\overline{k}) = \varphi(\overline{k}\cdot\overline{1}) = \varphi(k\overline{1}) = k\varphi(\overline{1}) = ka = \varphi_a(\overline{k})$. Thus by definition $\varphi = \varphi_a$. So for any $\varphi \in \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, A_n)$ we can find $a \in A_n$ such that $\Phi(a) = \varphi_a = \varphi$. Conclude by definition that $\Phi$ is surjective.

Now applying the First Isomorphism Theorem for $R$-modules we can conclude that $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, A_n) \cong A_n$. $\square$

**Exercise.** (DF §10.2 Exercise 5): Exhibit all $\mathbb{Z}$-module homomorphisms from $\mathbb{Z}/30\mathbb{Z}$ to $\mathbb{Z}/21\mathbb{Z}$.

*Proof.* By previous exercise we know $\mathrm{Hom}(\mathbb{Z}/30\mathbb{Z}, \mathbb{Z}/21\mathbb{Z}) \cong (\mathbb{Z}/21\mathbb{Z})_{30}$ where $(\mathbb{Z}/21\mathbb{Z})_{30} = \{a \in \mathbb{Z}/21\mathbb{Z} : 30a = 0\} = A_{30} = \{0, 7, 14\}$ and it has three elements. Hence we know that there are three homomorphisms from $\mathbb{Z}/30\mathbb{Z}$ to $\mathbb{Z}/21\mathbb{Z}$. The three homomorphisms are the ones defined by the trivial homomorphism, $\varphi_7(\overline{x}) = 7x$, $\varphi_{14}(\overline{x}) = 14x$. $\square$

**Exercise.** (DF §10.2 Exercise 6): Prove that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/(n,m)\mathbb{Z}$.

*Proof.* By previous exercise we know $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z})_n = \{a \in \mathbb{Z}/m\mathbb{Z} : na \equiv 0 \pmod{m}\}$. It will suffice to show that $A_n \cong \mathbb{Z}/(n,m)\mathbb{Z}$. Let $d = \gcd(n,m)$, so by definition there exist $a, b$ relatively prime, such that $n = ad$ and $m = bd$. Observe that $b \in A_n$ since

$$\begin{aligned}nb &=\equiv (ad)b \pmod{m}\\ &= a(bd) \pmod{m}\\ &= an \pmod{m}\\ &= 0 \pmod{m}\end{aligned}$$

Define $\varphi : \mathbb{Z} \to A_n$ by $\varphi(z) = zb \pmod{m}$. We must first show that this is in fact a $\mathbb{Z}$-module homomorphism. Let $z, y \in \mathbb{Z}$, $r \in \mathbb{Z}$ and observe that

$$\begin{aligned}\varphi(z+y) &= (z+y)b \pmod{m}\\ &= (zb + yb) \pmod{m}\\ &= zb \pmod{m} + yb \pmod{m}\\ &= \varphi(z) + \varphi(y)\end{aligned}$$

and

$$\begin{aligned}\varphi(rz) &= (rz) \pmod{m}\\ &= r\big(z \pmod{m}\big)\\ &= r\varphi(z)\end{aligned}$$

We must now show that $\varphi$ is surjective. Choose $t \in A_n$, by definition $nt \equiv 0 \pmod{m}$ and hence $m \mid nt$ or equivalently $bd \mid adt$ or equivalently $b \mid at$. Since $\gcd(a,b) = 1$, it must follow that $b \mid t$ so there exists $s \in \mathbb{Z}$ such that $t = sb$. Hence $\varphi(s) = sb \pmod{m} = t \pmod{m}$. Conclude that $\varphi$ is in fact surjective.

We will now show that $\ker\varphi = d\mathbb{Z}$. Observe that $\varphi(d) = db \pmod{m} \equiv m \pmod{m} \equiv 0 \pmod{m}$. So $d \in \ker\varphi$ and immediately $d\mathbb{Z} \subseteq \ker\varphi$. Now let $s \in \ker\varphi$. Then by definition $\varphi(s) = sb \pmod{m} \equiv 0 \pmod{m}$ so, by definition, $m \mod sb$ or equivalently $bd \mid sb$ or equivalently $d \mid s$ so $s \in d\mathbb{Z}$. Hence $\ker\varphi \subset d\mathbb{Z}$. Conclude that $\ker\varphi = d\mathbb{Z}$.

By the First Isomorphism Theorem for Modules we have $\mathbb{Z}/\ker\varphi \cong A_n$. Result follows by equality

$$\mathbb{Z}/\ker\varphi = \mathbb{Z}/d\mathbb{Z} = \mathbb{Z}/(n,m)\mathbb{Z} \cong A_n \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}). \quad \square$$

**Exercise.** (DF §10.2 Exercise 7): Let $z$ be a fixed element of the center of $R$. Prove that the map $m \to zm$ is an $R$-module homomorphism from $M$ to itself. Show that for a commutative ring $R$ the map from $R$ to $\operatorname{End}_R M$ given by $r \to rI$ is a ring homomorphism (where $I$ is the identity endomorphism).)

*Proof.* Recall that the center of $R$ is $\{z \in R : zr = rz \text{ for all } r \in R\}$. Let $z$ be in the center of $R$ then by definition $zr = rz$ for all $r \in R$. Define $\varphi : M \to M$ by $\varphi(m) = zm$. We claim that this is an $R$-module homomorphism. Let $m, m' \in M$, $r \in R$. Observe that $\varphi(m + m') = z(m + m')zm + zm' = \varphi(m) + \varphi(m')$ and $\varphi(rm) = zrm = rzm = r\varphi(m)$. Conclude by definition that $\varphi$ is in fact an $R$-module homomorphism.

*Note:* We are making the assumption that "$I$ being the identity endomorphism" means *multiplicative identity*. Now let $R$ be a commutative ring and define $\Phi : R \to \operatorname{End}_R(M)$ by $\Phi(r) = rI$ where $I : M \to M$, defined by $I(m) = m$, is the identity endomorphism. We want to show that $\Phi$ is a ring homomorphism. Let $r, s \in R$ and observe that for all $m \in M$

$$\begin{aligned}\Phi(r+s)(m) &= (r+s)I(m)\\ &= (r+s)m\\ &= rm + rs\\ &= rI(m) + sI(m)\\ &= \Phi(r)(m) + \Phi(s)(m)\end{aligned}$$

So by definition $\Phi(r + s) = \Phi(r) + \Phi(s)$. Moreover,

$$\begin{aligned}\Phi(rs) &= rsI(m)\\ &= rsI(m)I(m)\\ &= rI(m)\cdot sI(m)\\ &= \Phi(r)(m)\Phi(s)(m)\end{aligned}$$

And hence $\Phi(rs) = \Phi(r)\Phi(s)$ and we can conclude by definition that $\Phi$ is a ring homomorphism. □

**Exercise.** (DF §10.2 Exercise 8): Let $\varphi : M \to N$ be an $R$-module homomorphism. Prove that $\varphi(\operatorname{Tor}(M)) \subseteq \operatorname{Tor}(N)$.

*Proof.* Recall that $\operatorname{Tor}(M) = \{m \in M : rm = 0 \text{ for some } 0 \neq r \in R\}$. Now it follows that $\varphi(\operatorname{Tor}(M)) = \{n \in N : n = \varphi(m)$ for some $m \in \operatorname{Tor}(M)\}$. Let $n \in \varphi(\operatorname{Tor}(M))$ then $n = \varphi(m)$ for some $m \in \operatorname{Tor}(M)$ by definition. Since $m \in \operatorname{Tor}(M)$ there exists $0 \neq r \in R$ such that $rm = 0$. Hence $rn = r\varphi(m) = \varphi(rm) = \varphi(0) = 0$. Conclude that $n \in \operatorname{Tor}(N)$ and hence $\varphi(\operatorname{Tor}(M)) \subseteq \operatorname{Tor}(N)$. □

**Exercise.** (DF §10.2 Exercise 9): Let $R$ be a commutative ring. Prove that $\operatorname{Hom}_R(R, M)$ and $M$ are isomorphic as left $R$-modules.

*Proof.* Define $\Phi : \operatorname{Hom}_R(R, M) \to M$ by $\Phi(\varphi) = \varphi(1)$. We must first show that this is in fact an $R$-module homomorphism. Observe that for all $\varphi, \xi \in \operatorname{Hom}_R(R, M)$ and all $r \in R$ it follows that

$$\begin{aligned}\Phi(\varphi+\xi) &== (\varphi+\xi)(1)\\ &= \varphi(1) + \varphi(\xi)\\ &= \Phi(\varphi) + \Phi(\xi)\end{aligned}$$

and also by Proposition 2 we have

$$\begin{aligned}\Phi(r\varphi) &= (r\varphi)(1)\\ &= r\varphi(1)\\ &= r\Phi(\varphi)\end{aligned}$$

Hence we can now conclude that $\Phi$ is an $R$-module homomorphism.

We must now show that $\Phi$ is injective. Suppose that $\Phi(\varphi) = \Phi(\xi)$ then by definition $\varphi(1) = \xi(1)$ or equivalently $\varphi(1) - \xi(1) = 0$ and hence $(\varphi - \xi)(1) = 0$. But since $\varphi - \xi \in \operatorname{Hom}_R(R, M)$ it is an $R$-module homomorphism so $(\varphi - \xi)(x) = (\varphi - \xi)(x \cdot 1) = x(\varphi - \xi)(1) = x \cdot 0 = 0$ for all $x \in R$. Conclude that $\varphi(x) = \xi(x)$ for all $x \in R$ and hence by definition $\varphi = \xi$. Conclude that $\Phi$ is inective.

We must now show that $\Phi$ is surjective. Let $m \in M$ be arbitrary. We want to show that there exists $\varphi \in \operatorname{Hom}_R(R, M)$ such that $\Phi(\varphi) = m$. Let us define $\varphi : R \to M$ by $\varphi(x) = xm$. We need to show that $\varphi \in \operatorname{Hom}_R(R, M)$. Observe that $\varphi(x + y) = (x + y)m = xm + ym = \varphi(x) + \varphi(y)$ for all $x, y \in R$ and $\varphi(rx) = rxm = r\varphi(x)$ for all $x \in R$, $r \in R$. Hence we have shown that $\varphi$ is in fact an $R$-module homomorphism. Now observe that $\Phi(\varphi) = \varphi(1) = 1 \cdot m = m$. Conclude by definition that $\Phi$ is surjective.

We have shown that $\Phi$ is a bijective $R$-module homomorphism. Conclude that $\operatorname{Hom}_R(R, M) \cong M$. □

**Exercise.** (DF §10.2 Exercise 10): Let $R$ be a commutative ring. Prove that $\operatorname{Hom}_R(R, R)$ and $R$ are isomorphic as rings.

*Proof.* Define $\Phi : \mathrm{Hom}_R(R,R) \to R$ by $\Phi(\varphi) = \varphi(1)$. We will first show that $\Phi$ is a ring homomorphism. Observe that for all $\varphi, \xi \in \mathrm{Hom}_R(R,R)$ and all $r \in R$ by Proposition 2 we have

$$\begin{aligned}\Phi(\varphi+\xi) &= (\varphi+\xi)(1)\\ &= \varphi(1)+\xi(1)\\ &= \Phi(\varphi)+\Phi(\xi)\end{aligned}$$

and also by property of commutativity

$$\begin{aligned}\Phi(\varphi\circ\xi) &= (\varphi\circ\xi)(1)\\ &= \varphi(\xi(1))\\ &= \varphi(\xi(1)\cdot 1)\\ &= \xi(1)\varphi(1)\\ &= \varphi(1)\xi(1)\\ &= \Phi(\varphi)\Phi(\xi)\end{aligned}$$

Hence we can conclude that $\Phi$ is in fact a ring homomorphism.

We must now show that $\Phi$ is injective. Suppose that $\Phi(\varphi) = \Phi(\xi)$ then by definition $\varphi(1) = \xi(1)$ or equivalently $\varphi(1) - \xi(1) = 0$ and hence $(\varphi - \xi)(1) = 0$. But since $\varphi - \xi \in \mathrm{Hom}_R(R,R)$ it is an $R$-module homomorphism so $(\varphi-\xi)(x) = (\varphi-\xi)(x\cdot 1) = x(\varphi-\xi)(1) = x \cdot 0 = 0$ for all $x \in R$. Conclude that $\varphi(x) = \xi(x)$ for all $x \in R$ and hence by definition $\varphi = \xi$. Conclude that $\Phi$ is inective.

We must now show that $\Phi$ is surjective. Let $r \in R$ be arbitrary. We want to show that there exists $\varphi \in \mathrm{Hom}_R(R,R)$ such that $\Phi(\varphi) = r$. Let us define $\varphi : R \to R$ by $\varphi(x) = xr$. We need to show that $\varphi \in \mathrm{Hom}_R(R,R)$. Observe that $\varphi(x+y) = (x+y)r = xr + yr = \varphi(x) + \varphi(y)$ for all $x, y \in R$ and $\varphi(sx) = sxr = s\varphi(x)$ for all $s \in R$ and all $x \in R$. Hence we have shown that $\varphi$ is in fact an $R$-module homomorphism. Now observe that $\Phi(\varphi) = \varphi(1) = 1 \cdot r = r$. Conclude by definition that $\Phi$ is surjective.

We have shown that $\Phi$ is a bijective ring homomorphism. Conclude that $\mathrm{Hom}_R(R,R) \cong R$. $\square$

**Exercise.** (DF §10.2 Exercise 11): Let $A_1, A_2, \ldots, A_n$ be $R$-modules and let $B_i$ be submodules of $A_i$ for each $i = 1, 2, \ldots, n$. Prove that

$$(A_1 \times A_2 \times \cdots \times A_n)/(B_1 \times B_2 \times \cdots \times B_n) \cong (A_1/B_1) \times (A_2/B_2) \times \cdots \times (A_n/B_n).$$

*Proof.* Define $\varphi : A_1 \times A_2 \times \cdots \times A_n \to (A_1/B_1) \times (A_2/B_2) \times \cdots \times (A_n/B_n)$ by $\varphi(a_1, a_2, \ldots, a_n) = (a_1 + B_1, a_2 + B_2, \ldots, a_n + B_n)$. We want to show that this is an $R$-module homomorphism and that $\ker\varphi = B_1 \times B_2 \times \cdots \times B_n$ and that the mapping is surjective. Then the first isomorphism theorem for modules yields the result.

Let $x, y \in A_1 \times A_2 \times \cdots \times A_n$ where $x = (a_1, a_2, \ldots, a_n)$ and $y = (a_1', a_2', \ldots, a_n')$. Observe that

$$\begin{aligned}\varphi(x+y) &= \varphi((a_1, a_2, \ldots, a_n) + (a_1', a_2', \ldots, a_n'))\\ &= \varphi(a_1 + a_1', a_2 + a_2', \ldots, a_n + a_n')\\ &= (a_1 + a_1' + B_1, a_2 + a_2' + B_2, \ldots, a_n + a_n' + B_n)\\ &= (a_1 + B_1 + a_1' + B_1, a_2 + B_2 + a_2' + B_2, \ldots, a_n + B_n + a_n' + B_n)\\ &= (a_1 + B_1, a_2 + B_2, \ldots, a_n + B_n) + (a_1' + B_1, a_2' + B_2, \ldots, a_n' + B_n)\\ &= \varphi(a_1, a_2, \ldots, a_n) + \varphi(a_1', a_2', \ldots, a_n')\\ &= \varphi(x) + \varphi(y)\end{aligned}$$

and for $r \in R$

$$\begin{aligned}\varphi(rx) &= \varphi(r(a_1, a_2, \ldots, a_n))\\ &= \varphi(ra_1, ra_2, \ldots, ra_n)\\ &= (ra_1 + B_1, ra_2 + B_2, \ldots, ra_n + B_n)\\ &= (r(a_1 + B_1), r(a_2 + B_2), \ldots, r(a_n + B_n))\\ &= r(a_1 + B_1, a_2 + B_2, \ldots, a_n + B_n)\\ &= r\varphi(a_1, a_2, \ldots, a_n)\\ &= r\varphi(x)\end{aligned}$$

Thus by definition we can conclude that $\varphi$ is an $R$-moduel homomorphism.

Now we want to show that $\ker\varphi = B_1 \times B_2 \times \cdots \times B_n$. Observe that

$$\begin{aligned}\ker\varphi &= \{x \in A_1 \times A_2 \times \cdots \times A_n : \varphi(x) = 0\}\\ &= \{(a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \cdots \times A_n : \varphi(a_1, a_2, \ldots, a_n) = 0\}\end{aligned}$$

$$= \{(a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \cdots \times A_n : (a_1 + B_1, a_2 + B_2, \ldots, a_n + B_n) = (0, 0, \ldots, 0)\}$$
$$= \{(a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \cdots \times A_n : a_1 \in B_1, a_2 \in B_2, \ldots, a_n \in B_n\}$$

Hence $\ker\varphi \subseteq B_1 \times B_2 \times \cdots \times B_n$ and trivially $B_1 \times B_2 \times \cdots \times B_n \subseteq \ker\varphi$ by construction of $\varphi$. Conclude that $\ker\varphi = B_1 \times B_2 \times \cdots \times B_n$.

The mapping is trivially surjective. Applying first Isomorphism theorem yields the result. □

**Exercise.** (DF §10.3 Exercise 3): Show that the $F[x]$-modules in Exercises 18 and 19 of Section 1 are both cyclic.

*Proof.* For Problem 18: $F = \mathbb{R}$, $V = \mathbb{R}^2$, $T : V \to V$ is defined by $T(x, y) = (y, -x)$. Let $(a, b) \in \mathbb{R}^2$ be arbitrary. Observe that $(ax + b)(0, 1) = aT(0, 1) + b(0, 1) = a(1, 0) + b(0, 1) = (a, b)$. Hence it follows by definition that $V = \mathbb{R}(0, 1)$. Moreover it can also be written as $V = \mathbb{R}(1, 0)$ with $p(x) = a - bx$, so the representation is not unique.

For Problem 19: $F = \mathbb{R}$, $V = \mathbb{R}^2$, $T : V \to V$ is defined by $T(x, y) = (0, y)$. Let $(a, b) \in \mathbb{R}^2$ be arbitrary. Observe that $(a + (b - a)x)(1, 1) = (a, a) + (b - a)T(1, 1) = (a, a) + (0, b - a) = (a, b)$. Hence it follows by definition that $V = \mathbb{R}(1, 1)$. □

**Exercise.** (DF §10.3 Exercise 4): An $R$-module $M$ is called a *torsion* module if for each $m \in M$ there is a nonzero element $r \in R$ such that $rm = 0$, where $r$ may depend on $m$ (i.e., $M = \mathrm{Tor}(M)$ in the notation of Exercise 8 of Section 1). Prove that every finite abelian group is a torsion $\mathbb{Z}$-module. Give an example of an infinite abelian group that is a torsion $\mathbb{Z}$-module.

*Proof.* Let $M$ be a finite abelian group. Let $m \in M$. We want to show that there exists $0 \neq r \in R = \mathbb{Z}$ such that $rm = 0$. Consider $1m, 2m, 3m, 4m, \ldots$. These are not all distinct, because if they were we would have infinitely many, a contradiction. So we are assured $km = lm$ for some $k, l \in \mathbb{Z}$ nonzero with $k \neq l$. It follows that $km - lm = 0$ and hence by property of modules, $(k - l)m = 0$. Finally observe that $k - l \neq 0$ so $m \in \mathrm{Tor}(M)$. Conclude that $M = \mathrm{Tor}(M)$.

As for the example. Let $n \in \mathbb{Z}$ be greater than 1. Consider $A = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \cdots$ and observe that this is an infinite abelian group. This can be seen as a $\mathbb{Z}$-module. Let $(a_1, a_2, \ldots) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \cdots$ be arbitrary. Observe that $n(a_1, a_2, \ldots) = (na_1, na_2, \ldots) = (0, 0, \ldots) = \mathbf{0}$. □

**Exercise.** (DF §10.3 Exercise 5): Let $R$ be an intergral domain. Prove that every finitely generated torsion $R$-module has a nonzero annihilator i.e., there is a nonzero element $r \in R$ such that $rm = 0$ for all $m \in M$ – here $r$ does not depend on $m$ (the annihilator of a module was defined in Exercise 9 of Section 1). Give an example of a torsion $R$-module whose annihilator is the zero ideal.

*Proof.* Let $M$ be a finitely generated torsion $R$-module where $R$ is an integral domain. By definition $M = Rm_1 + \cdots + Rm_n$ for some $m_1, m_2, \ldots, m_n \in M$. Let $m \in M$. Since $M$ is finitely generated there exist $r_1, r_2, \ldots, r_n \in R$ such that $m = r_1m_1 + \cdots + r_nm_n$. Since $M$ is torsion, there exists $0 \neq \overline{r_i} \in R$ such that $\overline{r_i}m_i = 0$ for $i = 1, 2, \ldots, n$. Define $r = \overline{r_1}\overline{r_2} \cdots \overline{r_n}$. Now observe that

$$\begin{aligned} rm &= r(r_1m_1 + \cdots + r_nm_n) \\ &= (r_1\overline{r_2} \cdots \overline{r_n})\overline{r_1}m_1 + \cdots + (\overline{r_1} \cdots \overline{r_{n-1}}r_n)\overline{r_n}m_n \\ &= (r_1\overline{r_2} \cdots \overline{r_n}) \cdot 0 + \cdots + (\overline{r_1} \cdots \overline{r_{n-1}}r_n) \cdot 0 \\ &= 0 \end{aligned}$$

hence it follows that $0 \neq r \in \mathrm{Ann}(m)$ and thus $\mathrm{Ann}(m) \neq 0$.

As for the example: recall that $\mathbb{Q}$ is not finitely generated, and hence $\mathbb{Q}/\mathbb{Z} = m$ is also not finitely generated. observe that $m$ is torsion since for any rational, non-integer number $x$, multiplication by its denominator, which **is** an integer, yields an integer, which in this case would be 0 in $M$. Suppose by way of contradiction that there is a nonzero annihilator, say $0 \neq a \in R = \mathbb{Z}$. Choose $b \in \mathbb{Z}$ such that $b \nmid a$. Now $a \cdot 1/b = 0$ by property of being annihilator so $a/b = k$ is an integer. But then $a = bk$ and hence $b \mid a$, a contradiction. So there are no nonzero annihilators. □

**Exercise.** (DF §10.3 Exercise 9): An $R$-module $M$ is called *irreducible* if $M \neq 0$ and if 0 and $M$ are the only submodules of $M$. Show that $M$ is irreducible if and only if $M \neq 0$ and $M$ is a cyclic module with any nonzero element as its generator. Determine all the irreducible $\mathbb{Z}$-modules.

*Proof.* Suppose $M$ is irreducible. By definition $M \neq 0$. Let $0 \neq m \in M$. Note that $Rm \subseteq M$ is a nonzero since $1m = m \in Rm$. Since $M$ is irreducible and we have already shown $Rm \neq 0$, conclude that $Rm = M$ for any $0 \neq m \in M$.

Conversely suppose that $M \neq 0$ and $M$ is a cyclic module with any nonzero element as generator. Let $N$ be a submodule of $M$, so $0 \subseteq N \subseteq M$. If $N = 0$ we are done, so suppose $N \neq 0$, then there exists $n \in N$ such that $n \neq 0$. But $n \in M$ and so $M = Rn$. Since $Rn \subseteq N$ immediately we have just shown $M \subseteq N$. Since both $N \subseteq M$ and $M \subseteq N$ we have $M = N$.

Let $M$ be an irreducible $\mathbb{Z}$-module then $M$ is cyclic as an abelian group and moreover $M$ has finite order. Since it has only two subgroups, the trivial one and the whole group itself, we can conclude that the irreducible $\mathbb{Z}$ modules are of the form $\mathbb{Z}/p\mathbb{Z}$ where $p$ is prime. □

**Exercise.** (DF §10.3 Exercise 10): Assume $R$ is commutative. Show that an $R$-module $M$ is irreducible if and only if $M$ is isomorphic (as an $R$-module) to $R/I$ where $I$ is a maximal ideal of $R$. [By the previous exercise, if $M$ is irreducible there is a natural map $R \to M$ defined by $r \mapsto rm$, where $m$ is any fixed nonzero element of $M$.]

*Proof.* Let $M$ be an $R$-module. Suppose $M$ is irreducible. Then by definition $M \neq 0$ and the only submodules of $M$ are 0 and $M$. Define $\varphi_m : R \to M$ by $\varphi(r) = rm$ where $0 \neq m$ is a fixed element of $M$. We want to show that this is in fact an $R$-module homomorphism. Let $x, y \in R$ and $r \in R$ and observe that $\varphi(x+y) = (x+y)m = xm + ym = \varphi(x) + \varphi(y)$ and $\varphi(rx) = rxm = r\varphi(x)$. This mapping is surjective since $M$ is a cyclic module with any nonzero element as its generator. So by the First Isomorphism Theorem for Modules, it follows that $R/\ker\varphi_m \cong M$. $\ker\varphi_m$ is a submodule by a previous exercise and is trivially an ideal of $R$. It will suffice to show that $\ker\varphi_m$ is a maximal ideal for the result to follow. Let $0 \neq \overline{r} \in R/\ker\varphi_m$ where $\overline{r} = r + \ker\varphi_m$. It follows that $\varphi_m(r) = rm \neq 0$. We want to show that $\overline{r}$ has a multiplicative inverse. Since $M$ is irreducibleand $rm \neq 0$, we have $M = R(rm)$ by previous exercise. In particular $m = s(rm)$ for some $s \in R$. Then by equality $1 \cdot m - (sr)m = 0$ resulting in $(1 - sr) \in \ker\varphi_m$, By property of cosets, we have $1 + \ker\varphi_m = sr + \ker\varphi_m = (s + \ker\varphi_m)(r + \ker\varphi_m)$. We have just shown that $\overline{1} = \overline{s} + \overline{r}$ giving us $\overline{s}$ as the multiplicative inverse of $\overline{r}$, an arbitrary nonzero element (by commutativity of $R$, it is both a left and right inverse). Thus $R/\ker\varphi_m$ is a field and so $\ker\varphi_m$ is a maximal ideal.

Conversely suppose $M \cong R/I$ where $I$ is a maximal ideal of $R$ (as an $R$-module homomorphism). Then by definition there exists $\varphi : M \to R/I$ such that $\varphi(m+n) = \varphi(m) + \varphi(n)$ and $\varphi(rm) = r\varphi(m)$ for all $m, n \in M$, $r \in R$. Observe that $M \neq 0$ since $M \cong R/I$ and $I$ is maximal, by definition $I \neq R$ so $R/I$ cannot be trivially 0 so $M$ cannot be trivially 0. Suppose $N$ is a submodule of $M$, then $0 \subseteq N \subseteq M$. Suppose, by way of contradiction, that $0 \neq N \neq M$. Note that $\varphi(N)$ is a submodule of $R/I$ and trivially $\varphi(N)$ is an ideal of $R/I$ which is not 0 and not $R/I$ a contradiction to $0 \neq N \neq M$ since $R/I$ is a field, the only ideals of $R/I$ are 0 and $R/I$. So either $0 = N$ or $N = M$. Conclude by definition that $M$ is irreducible. □

**Exercise.** (DF §10.3 Exercise 15): An element $e \in R$ is called a *central idempotent* if $e^2 = e$ and $er = re$ for all $r \in R$. If $e$ is a central idempotent in $R$, prove that $M = eM \oplus (1-e)M$. [Recall Exercise 14 in Section 1.]

*Proof.* Suppose $r$ is a central idempotent in $R$. We want to show that $M = eM \oplus (1-e)M$, that is, any $m \in M$ can be written *uniquely* of the form $em_1 + (1-e)m_2$ for some $m_1, m_2 \in M$. Let $m \in M$ and observe that $m = em + (m - em)$ so $M \subseteq eM + (1-e)M$ and $eM + (1-e)M \subseteq M$ trivially by closure of modules. Now we need to show the uniqueness. Suppose $m \in eM \cap (1-e)M$ then $m = em_1 = (1-e)m_2$ for some $m_1, m_2 \in M$. But then $em_1 = m_2 - em_2$ or equivalently $e(m_1 + m_2) = m_2$. Multiplying both sides by $e$, we get $e^2(m_1 + m_2) = em_2$ and since $e^2 = e$ we have $em_1 + em2 - em_2 = em_1 = 0$. Hence $m = 0$. Conclude that $eM \cap (1-e)M = 0$. □

**Exercise.** (DF §10.3 Exercise 16): For any ideal $I$ of $R$ let $IM$ be the submodule defined in Exercise 5 of Section 1. Let $A_1, \ldots, A_k$ be any ideals in the ring $R$. Prove that the map

$$M \to M/A_1M \times \cdots \times M/A_kM \text{ defined by } m \mapsto (m + A_1M, \ldots, m + A_kM)$$

is an $R$-module homomorphism with kernel $A_1M \cap A_2M \cap \cdots \cap A_kM$.

*Proof.* We first must show that $\varphi : M \to M/A_1M \times \cdots \times M/A_kM$ defined by $\varphi(m) = (m + A_1M, \ldots, m + A_kM)$ is in fact an $R$-module homomorphism. Let $m_1, m_2 \in M$, $r \in R$. Observe that

$$\begin{aligned}
\varphi(m_1 + m_2) &= (m_1 + m_2 + A_1M, \ldots, m_1 + m_2 + A_kM) \\
&= \big((m_1 + A_1M) + (m_2 + A_1M), \ldots, (m_1 + A_kM) + (m_2 + A_kM)\big) \\
&= (m_1 + A_1M, \ldots, m_1 + A_kM) + (m_2 + A_1M, \ldots, m_2 + A_kM) \\
&= \varphi(m_1) + \varphi(m_2)
\end{aligned}$$

and

$$\begin{aligned}
\varphi(rm_1) &= (rm_1 + A_1M, \ldots, rm_2 + A_kM) \\
&= \big(r(m_1 + A_1M), \ldots, r(m_1 + A_kM)\big) \\
&= r(m_1 + A_1M, \ldots, m_1 + A_kM) \\
&= r\varphi(m_1)
\end{aligned}$$

Now by the First Isomorphism Theorem for Modules we have $M/\ker\varphi \cong \varphi(M)$ where

$$\begin{aligned}
\ker\varphi &= \{m \in M : \varphi(m) = 0\} \\
&= \{m \in M : (m + A_1M, \ldots, m + A_kM) = (0, \ldots, 0)\} \\
&= \{m \in M : m \in A_1M, \ldots, m \in A_kM\} \\
&= A_1M \cap \cdots \cap A_kM
\end{aligned}$$

□

**Exercise.** (DF §10.3 Exercise 22): Let $R$ be a Principal Ideal Domain, let $M$ be a torsion $R$-module (cf. Exercise 4) and let $p$ be a prime in $R$ (do not assume $M$ is finitely generated, hence it need not have a nonzero annihilator – cd. Exercise 5). The *$p$-primary component* of $M$ is the set of all elements of $M$ that are annihilated by some positive power of $p$.

(1) Prove that the $p$-primary component is a submodule. [See Exercise 13 in Section 1.]

*Proof.* Let $A$ be the $p$-primary component, i.e., $A = \{m \in M : p^i m = 0 \text{ for some } i \in \mathbb{N}\}$. Observe that $pm = 0$ for $m = 0$ so $A \neq \emptyset$. Let $m, n \in A$, $r \in R$ a PID. Since $m \in A$ there exists $i \in \mathbb{N}$ such that $p^i m = 0$. Since $n \in A$ there exists $j \in \mathbb{N}$ such that $p^j n = 0$. Choose $l = \min\{i, j\}$ and observe that

$$\begin{aligned} p^l(m + rn) &= p^l m + rp^l n \\ &= p^{l-i}(p^i m) + rp^{l-j}(p^j n) \\ &= p^{l-i} \cdot 0 + rp^{l-j} \cdot 0 \\ &= 0 \end{aligned}$$

Conclude that $m + rn \in A$ and thus by the Submodule Criterion, $A$ is in fact a submodule. □

(2) Prove that this definition of $p$-primary component agrees with the one given in Exercise 18 when $M$ has a nonzero annihilator.

*Proof.* Suppose $\text{Ann}(M) \neq 0$, then there exists $0 \neq a \in \text{Ann}(M)$ such that $\text{Ann}(M) = (a)$ since $R$ is a Principal Ideal Domain. Since every PID is a UFD and primes are irreducibles in here, we can decompose $a$, say $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$. We want to show that $M_{p_i} = \{m \in M : p_i^j m = 0 \text{ for some } j \in \mathbb{N}\}$ is equal to $M_i = \{m \in M : p_i^{\alpha_i} m = 0\}$.

Let $m \in M_i$, then by definition we know that $p_i^{\alpha_i} m = 0$ and immediately it follows that $m \in M_{p_i}$. Conclude that $M_i \subseteq M_{p_i}$.

Conversely suppose that $m \in M_{p_i}$ then by definition there exists $j \in \mathbb{N}$ such that $p_i^j m = 0$. Consider $(a, p_i^j)$ and observe that since $R$ is a PID, it must follow that $(a, p_i^j) = (b)$ for some $b \in R$. But also note that $(p_i^j) \subseteq (a, p_i^j) = (b)$, so by property of ideals, we have $b \mid p_i^j$ which leads us to conclude by property of primes that $b = p_i^t$ for some $t \leq j$. But we also know that $(a) \subseteq (p_i^t)$ so it follows that

$$\begin{aligned} p_i^t &\mid p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_i^{\alpha_i} p_{i+1}^{\alpha_{i+1}} \cdots p_n^{\alpha_n} \\ p_i^{t-\alpha_i} p_i^{\alpha_i} &\mid p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_i^{\alpha_i} p_{i+1}^{\alpha_{i+1}} \cdots p_n^{\alpha_n} \\ p_i^{t-\alpha_i} &\mid p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_n^{\alpha_n} \end{aligned}$$

So by definition $p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_n^{\alpha_n} = p_i^{t-\alpha_i} s$ for some $s \in R$. It must follow that $t - \alpha_i = 0$, or equivalently $t = \alpha_i$, because if it does not, we have a contradiction, since $p_i$ is not in $\{p_1, \ldots, p_{i-1}, p_{i+1}, \ldots, p_n\}$. So since $(p_i^j) \subseteq (a, p_i^j) = (p_i^{\alpha_i})$ we have $p_i^{\alpha_i} = p_i^j \cdot k$ for some $k \in R$. So $p_i^{\alpha_i} m = p_i^j \cdot k \cdot m = k \cdot (p_i^j \cdot m) = k \cdot 0 = 0$. Conclude that $m \in M_i$ and hence $M_{p_i} \subseteq M_i$.

Finally, by double inclusion, we can conclude that $M_i = M_{p_i}$. □

(3) Prove that $M$ is the (possibly infinite) direct sum of its $p$-primary components, as $p$ runs over all primes of $R$.

Department of Mathematics, California State University Long Beach
*E-mail address*: mrrobertcardona@gmail.com and massy255@gmail and siavash.mortezavi@gmail