Solutions 10

1. A module is ***simple*** if it is not the zero module and if it has no proper submodule.

i. Let V be a simple R-module. Show that V is cyclic.

ii. Prove *Schur's Lemma*: Any R-linear map $\varphi : V \to W$ between simple R-modules is either is zero or an isomorphism.

iii. For a simple R-module V, show that the set $\operatorname{End}_R(V)$ of endomorphisms forms a field where multiplication is given by composition of functions and addition is defined pointwise.

Solution.

i. A nonzero element g in V generates a nonzero submodule $\langle g \rangle$ in V. As V is simple, it follows that $V = \langle g \rangle$.

ii. Since V is simple, the submodule $\operatorname{Ker}(\varphi) \subseteq V$ is either 0 or V, so φ is either injective or the zero map. Since W is simple, the submodule $\operatorname{Im}(\varphi) \subseteq W$ is either 0 or W, so φ is either the zero map or surjective. Combining these, we see that φ is either zero or an isomorphism.

iii. The set $\operatorname{End}_R(V)$ forms an R-module where is addition defined pointwise, so it is an abelian group under addition. For any φ, ψ, and θ in $\operatorname{End}_R(V)$ and any v in V, we have

$$\big(\varphi \circ (\psi + \theta)\big)(v) = \varphi\big((\psi + \theta)(v)\big) = \varphi\big(\psi(v) + \theta(v)\big) = (\varphi \circ \psi)(v) + (\varphi \circ \theta)(v)\,,$$

so the distributive axiom holds. Because V is a simple module, part *ii* implies that the set of endomorphism consists of the zero map and the set of R-module automorphisms $\operatorname{Aut}_R(V)$ of V. As the set $\operatorname{Aut}_R(V)$ is a group, it follows that multiplication in $\operatorname{End}_R(V)$ is associative with the identity $\mathrm{id}_V : V \to V$ and any nonzero element is a unit. Finally, part *i* implies that $V = \langle u \rangle$ for some u in V. For any v in V, there exists r in R such that $v = r\,u$. For any φ and ψ in $\operatorname{End}_R(V)$, define s and t in R by $\varphi(u) := s\,u$ and $\psi(u) := t\,u$. Hence, we have

$$(\varphi \circ \psi)(v) = r\,\varphi\big(\psi(u)\big) = r\,t\,\varphi(u) = r\,t\,s\,u = r\,s\,\psi(u) = r\,\psi\big(\varphi(u)\big) = (\psi \circ \varphi)(v)\,,$$

so $\varphi \circ \psi = \psi \circ \varphi$ and the multiplication is commutative. Therefore, $\operatorname{End}_R(V)$ is a field. □

2. Let R be domain and let V be an R-module. An element v in V is a ***torsion element*** if there is a nonzero element r in R such that $r\,v = 0$. Let $\tau(V)$ be the set of torsion elements of V. A module V is ***torsion*** if $\tau(V) = V$ and it is ***torsion-free*** if $\tau(V) = 0$.

i. Demonstrate that the ***annihilator*** $\operatorname{Ann}(V) := \{f \in R \mid f\,v = 0 \text{ for all } v \in V\}$ forms an ideal in R.

ii. Show that $\tau(V)$ is a submodule of V.

iii. Prove that $V/\tau(V)$ is torsion-free.

iv. For any R-linear map $\varphi : V \to W$, demonstrate that $\varphi\big(\tau(V)\big) \subseteq \tau(W)$.

v. Give an example of an infinite abelian group that is a torsion $\mathbb{Z}$-module.

Solution.

i. For any r and s in R, any f and g in $\operatorname{Ann}(V)$, and any v in V, we have

$$(r\,f + s\,g)\,v = r\,(f\,v) + s\,(g\,v) = r\,0 + s\,0 = 0\,,$$

so $r\,f + s\,g \in \operatorname{Ann}(V)$ and the annihilator of V is an ideal in R.

ii. By definition, an element v in R is a torsion element if $\operatorname{Ann}(v) \neq 0$. Suppose that v and v' are elements in $\tau(V)$. There exists nonzero elements r and r' in R such that $r\,v = 0$ and $r'\,v' = 0$. For any s and s' in R, we have

$$r\,r'\,(s\,v + s\,v') = s\,r'\,(r\,v) + s'\,r\,(r'\,v') = s\,r'\,0 + s'\,r\,0 = 0\,.$$

As R is domain, we have $r\,r' \neq 0$ and $\operatorname{Ann}(s\,v + s\,v') \neq 0$. Thus, we deduce that $s\,v + s'\,v' \in \tau(V)$, so $\tau(V)$ is a submodule.

iii. Choose an element u in V such that the coset $u + \tau(V)$ in $V/\tau(V)$ is nonzero; this means u is not in $\tau(V)$ and $\operatorname{Ann}(u) = 0$. Suppose that $\operatorname{Ann}\big(u + \tau(V)\big) \neq 0$. It follows that there exists a nonzero element r in R such that

$$0 = r\big(u + \tau(V)\big) = r\,u + \tau(M)\,,$$

so we deduce that $r\,u \in \tau(V)$. Hence, there exist a nonzero element r' in R such that $0 = r'\,(r\,u) = (r'\,r)\,u$. As R is a domain, we have $r'\,r \neq 0$. It follows that $\operatorname{Ann}(u) \neq 0$ contradicting the hypothesis that $u + \tau(V) \neq 0$. We conclude that $\tau\big(V/\tau(V)\big) = 0$ and $V/\tau(V)$ is torsion-free.

iv. Consider an element v in $\tau(V)$; there exists a nonzero element r in R such that $r\,v = 0$. Applying the R-linear map φ, we obtain $0 = \varphi(r\,v) = r\,\varphi(v)$, which shows that $\varphi(v) \in \tau(W)$.

v. For any integer p and any nonzero integer q, we have

$$q(p/q + \mathbb{Z}) = p + \mathbb{Z} = 0$$

in $\mathbb{Q}/\mathbb{Z}$. Hence, every element in $\mathbb{Z}$-module $\mathbb{Q}/\mathbb{Z}$ is a torsion element and $\mathbb{Q}/\mathbb{Z}$ is a torsion module. Because $\{1/q + \mathbb{Z} \mid 0 < q \in \mathbb{Z}\}$ is a distinct set of elements in $\mathbb{Q}/\mathbb{Z}$, we see that $\mathbb{Q}/\mathbb{Z}$ is an infinite abelian group. □

3. *i.* Let $\varphi\colon V' \to V$ and $\psi\colon V \to V''$ be R-linear maps. Prove that the sequence

$$(\ddagger) \qquad V' \xrightarrow{\ \varphi\ } V \xrightarrow{\ \psi\ } V'' \longrightarrow 0$$

is exact if and only if, for every R-module W, the sequence

$$(\bigstar) \qquad 0 \longrightarrow \operatorname{Hom}_R(V'', W) \xrightarrow{\operatorname{Hom}_R(\psi, W)} \operatorname{Hom}_R(V, W) \xrightarrow{\operatorname{Hom}_R(\varphi, W)} \operatorname{Hom}_R(V', W)$$

is exact.

ii. Show that $\operatorname{Hom}_{\mathbb{Z}}\big(\mathbb{Z}/\langle m\rangle, \mathbb{Z}/\langle n\rangle\big) \cong \mathbb{Z}/\langle d\rangle$ where $d := \gcd(m, n)$.

Solution.

i. Suppose that the sequence $(\ddagger)$ is exact. Given an R-linear map $\varsigma\colon V'' \to W$ such that $\big(\operatorname{Hom}_R(\psi, W)\big)(\varsigma) = \varsigma \circ \psi = 0$, it follows that $\varsigma = 0$ because ψ is surjective. Hence, the sequence $(\bigstar)$ is exact at $\operatorname{Hom}_R(V'', W)$. As $\psi \circ \varphi = 0$, it follows that

$$\operatorname{Hom}_R(\varphi, W) \circ \operatorname{Hom}_R(\psi, W) = \operatorname{Hom}_R(\psi \circ \varphi, W) = \operatorname{Hom}_R(0, W) = 0$$

which shows that $\operatorname{Im}(\operatorname{Hom}_R(\varphi, W)) \subseteq \operatorname{Ker}(\operatorname{Hom}_R(\psi, W))$. Consider an R-linear map $\theta \colon V \to W$ in $\operatorname{Ker}(\operatorname{Hom}_R(\varphi, W))$. As $\theta \circ \varphi = 0$, we have $\operatorname{Ker}(\theta) \supseteq \operatorname{Im}(\varphi)$. The sequence (‡) being exact guarantees that $\operatorname{Im}(\varphi) = \operatorname{Ker}(\psi)$ which implies that $\operatorname{Ker}(\theta) \supseteq \operatorname{Ker}(\psi)$. Since ψ is surjective, there exists an R-linear map $\theta' \colon V'' \to W$ such that $\theta = \theta' \circ \psi = (\operatorname{Hom}_R(\psi, W))(\theta')$ and we deduce that

$$\operatorname{Ker}(\operatorname{Hom}_R(\varphi, W)) \subseteq \operatorname{Im}(\operatorname{Hom}_R(\psi, W))$$

which completes the proof that the sequence (★) is exact.

Suppose that, for any R-module W, the sequence (★) is exact. Since

$$\operatorname{Hom}_R(\varphi, W) \circ \operatorname{Hom}_R(\psi, W) = 0\,,$$

it follows that, for any R-linear map $\theta \colon V'' \to W$, we have $\theta \circ \psi \circ \varphi = 0$. Taking $W = V''$ and setting $\theta = \mathrm{id}_{V''}$, we see that $\psi \circ \varphi = 0$ and $\operatorname{Im}(\varphi) \subseteq \operatorname{Ker}(\psi)$. Similarly, taking $W = \operatorname{Coker}(\varphi)$ and letting $\pi \colon V \to W = V/\operatorname{Im}(\varphi)$ be the canonical map, we obtain $(\operatorname{Hom}_R(\varphi, W))(\pi) = \pi \circ \varphi = 0$, which implies that π in $\operatorname{Ker}(\operatorname{Hom}_R(\varphi, W))$. Since $\operatorname{Ker}(\operatorname{Hom}_R(\varphi, W)) = \operatorname{Im}(\operatorname{Hom}_R(\psi, W))$, there exists an R-linear map $\rho \colon V'' \to W$ satisfying $\pi = (\operatorname{Hom}_R(\psi, W))(\rho) = \rho \circ \psi$. In particular, we have $\operatorname{Im}(\varphi) = \operatorname{Ker}(\pi) \supseteq \operatorname{Ker}(\psi)$ which proves that the sequence (‡) is exact at V. Finally, taking $W := V''/\operatorname{Im}(\psi)$ and letting $\eta \colon V'' \to W$ be the canonical map gives $(\operatorname{Hom}_R(\psi, W))(\eta) = \eta \circ \psi = 0$. Because $\operatorname{Hom}_R(\psi, W)$ is injective, it follows that $\eta = 0$. We conclude that $W = 0$, ψ is surjective, and the sequence (‡) is exact at V'.

ii. Let $\mu \colon \mathbb{Z} \to \mathbb{Z}$ be the $\mathbb{Z}$-linear map defined by $\mu(1_{\mathbb{Z}}) = m$ and let $\pi \colon \mathbb{Z} \to \mathbb{Z}/\langle m \rangle$ be the canonical map. Hence, we have an exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\ \mu\ } \mathbb{Z} \xrightarrow{\ \pi\ } \frac{\mathbb{Z}}{\langle m \rangle} \longrightarrow 0\,.$$

When $W := \mathbb{Z}/\langle n \rangle$, part i gives

$$0 \longrightarrow \operatorname{Hom}_{\mathbb{Z}}\left(\frac{\mathbb{Z}}{\langle m \rangle}, \frac{\mathbb{Z}}{\langle n \rangle}\right) \xrightarrow{\operatorname{Hom}_{\mathbb{Z}}(\pi, \mathbb{Z}/\langle n \rangle)} \operatorname{Hom}_{\mathbb{Z}}\left(\mathbb{Z}, \frac{\mathbb{Z}}{\langle n \rangle}\right) \xrightarrow{\operatorname{Hom}_{\mathbb{Z}}(\mu, \mathbb{Z}/\langle n \rangle)} \operatorname{Hom}_{\mathbb{Z}}\left(\mathbb{Z}, \frac{\mathbb{Z}}{\langle n \rangle}\right)$$

The canonical isomorphism $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/\langle n \rangle) \cong \mathbb{Z}/\langle n \rangle$ identifies the R-linear map $\theta \colon \mathbb{Z} \to \mathbb{Z}/\langle n \rangle$ with the element $\theta(1_{\mathbb{Z}})$ in $\mathbb{Z}/\langle n \rangle$. Hence, it follows that $(\theta \circ \mu)(1_{\mathbb{Z}}) = \theta(m) = m\,\theta(1_{\mathbb{Z}})$ and

$$0 \longrightarrow \operatorname{Hom}_{\mathbb{Z}}\left(\frac{\mathbb{Z}}{\langle m \rangle}, \frac{\mathbb{Z}}{\langle n \rangle}\right) \longrightarrow \frac{\mathbb{Z}}{\langle n \rangle} \xrightarrow{\ \mu^*\ } \frac{\mathbb{Z}}{\langle n \rangle}$$

where $\mu^*(i) = m\,i$. We obtain $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/\langle m \rangle, \mathbb{Z}/\langle n \rangle) \cong \operatorname{Ker}(\mu^*)$.

Set $d := \gcd(m, n)$ and write $n = n'\,d$ for some integer n'. We have $\mu^*(i) = 0$ if and only if n divides $m\,i$; equivalently n' divides i. Therefore, we conclude that $\operatorname{Ker}(\mu^*) = n'\,(\mathbb{Z}/\langle n \rangle) \cong \mathbb{Z}/\langle d \rangle$ as required. □