Suggested Exercises Section 2 Solutions

Exercise 2.1. Let R be a commutative ring, let M be an R-module and let I be an ideal of R. Suppose that $IM = \{\sum_{\text{finite}} a_i x_i \mid a_i \in I,\ x_i \in M\} = 0$. Define a structure of R/I-module on M.

Solution. Define

$$(a+I)x = ax, \quad \text{for all } a \in R \text{ and all } x \in M.$$

By assumption, this is well defined, since for all $a \in I$ and all $x \in M$, we have $ax = 0$. A routine check shows that the module axioms hold.

A more elegant way to see this is that the R-module structure map $\rho : R \to \operatorname{End}_R(M)$ factors through R/I (or more precisely through the quotient map $\pi : R \to R/I$, which is a ring homomorphism). That is, ρ defines a ring homomorphism $\overline{\rho} : R/I \to \operatorname{End}_R(M)$ such that the diagram

$$\begin{tikzcd} R \arrow[rr, "\rho"] \arrow[dr, "\pi"'] & & \operatorname{End}_R(M) \\ & R/I \arrow[ur, "\overline{\rho}"'] & \end{tikzcd} \quad \text{commutes.}$$

Exercise 2.2. Recall that a $\mathbb{Z}$-module is the same as an abelian group. Determine the group structure of $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Z}/n)$ as an abelian group, for all integers $m, n \geq 2$. More generally, let R be a commutative ring and I, J two ideals of R. Describe $\operatorname{Hom}_R(R/I, R/J)$ as an R-module.

Solution. We use that $\operatorname{Hom}_R(R, M)$ is an R-module isomorphic to M shown previously, and show that $\operatorname{Hom}_R(R/I, R/J) \cong R/I + J$ as R-module. Namely, observe that

$$\operatorname{Hom}_R(R/I, R/J) \cong \{\varphi \in \operatorname{Hom}_R(R, R/J) \mid I = \ker(\varphi)\} \cong (R/J)\big/(I + J/J) \cong R/I + J,$$

where the first and last isomorphisms are consequences of the (first) isomorphism theorem (for modules and for rings), and the second isomorphism follows from the previous exercise. In particular, the isomorphism $\operatorname{Hom}_R(R/I, R/J) \cong R/I + J$ is as R-modules.

In particular $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Z}/n) \cong \mathbb{Z}/\big((m) + (n)\big) = \mathbb{Z}/\gcd(m, n)$ as abelian groups (with our usual abuse of notation $\mathbb{Z}/n = \mathbb{Z}/(n)$).

Exercise 2.3. Let R be a commutative ring and let M, N be two R-modules. Verify that $\operatorname{Hom}_R(M, N)$ is an R-module for the R-action $(af)(x) = af(x)$ for all $a \in R, f \in \operatorname{Hom}_R(M, N)$ and $x \in M$. How can you generalise the construction to arbitrary rings and left modules?

Solution. Recall that $\operatorname{Hom}_R(M, N)$ is an abelian group for the pointwise addition of maps, and with additive identity element the zero map. We check the axioms for an R-module, which is routine. E.g. for $a \in R, f, g \in \operatorname{Hom}_R(M, N)$, then for all $x \in M$ we have by definition

$$(a(f+g))(x) = (f+g)(ax) = f(ax) + g(ax) = af(x) + ag(x) = a(f(x) + g(x)) = (af + ag)(x),$$

showing that $a(f+g) = af + ag$.

Similarly for $(a+b)f = af + bf$, $(ab)f = a(bf)$ and $1f = f$ for all $a, b \in R$ and all $f, g \in \operatorname{Hom}_R(M, N)$.

If R is not commutative, and M, N are left R-modules, then we can regard $\operatorname{Hom}_R(M, N)$ as an abelian group but not an R-module, unless R is a group algebra, for instance. We refer the student interested in this deviation from our topic to Lang's Algebra, Section III.2.

Exercise 2.4. Let M be an R-module.

i. Prove that the torsion subgroup $M_{\mathbb{Z}-tor}$ of M, formed by the elements of finite order, is an R-module.

ii. Suppose that R is a commutative ring.

   (a) Prove that the (R-)torsion submodule $M_{tor} = \{x \in M \mid \exists\, a \in R,\ a \neq 0,$ such that $ax = 0\}$ is an R-submodule of M.

   (b) Prove that $\big(M/M_{tor}\big)_{tor} = \{0\}$.

iii. Find an example of (non-commutative) ring R and R-module M for which M_{tor} is not an R-submodule of M.

Solution.

i. By definition, $M_{\mathbb{Z}-tor}$ is a subgroup of M since $\mathbb{Z}$ is abelian. Let $a \in R$ and $x \in M_{\mathbb{Z}-tor}$. Suppose that $nx = 0$ with $n \in \mathbb{Z},\ n \neq 0$. Then (since every ring is a $\mathbb{Z}$-algebra), $n(ax) = a(nx) = 0$. Hence $ax \in M_{\mathbb{Z}-tor}$.

ii. Suppose that R is a commutative ring.

   (a) We first show that the set $M_{tor} = \{x \in M \mid \exists\, a \in R,\ a \neq 0,$ such that $ax = 0\}$ is a subgroup of M. Note that $M_{tor} \neq \emptyset$ since $0 \in M_{tor}$. Let $x, y \in M_{tor}$, and let $a, b \in R$ with $a, b \neq 0$ and $ax = by = 0$. Then, since R is commutative, $(ab)(x - y) = b(ax) - a(by) = 0$. So M_{tor} is a subgroup of M. Moreover, by commutativity of R, given $x \in M_{tor}$ and $0 \neq a \in R$ such that $ax = 0$, then for all $b \in R$ we have $a(bx) = b(ax) = 0$. That is, $Rx \subseteq M_{tor}$ for all $x \in M_{tor}$.

   (b) Let $x + M_{tor} \in M/M_{tor}$. If $0 \neq a \in R$ is such that $ax \in M_{tor}$, then there exists $0 \neq b \in R$ such that $0 = b(ax) = (ba)x$, showing that $x \in M_{tor}$.

iii. We claim that M_{tor} is in not a subgroup in general. Let $R = M_2(\mathbb{R})$ be the ring of 2×2 matrices with real coefficients, and let $M = R$. Let $x = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ and $y = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Then $xy = yx = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0_R$, and so $x, y \in M_{tor}$. But $x + y = 1_R$ is not in M_{tor} since $a1 = a$.

Exercise 2.5. Let R be a commutative ring. The *annihilator* of an R-module M is $\mathrm{Ann}(M) = \{a \in R \mid ax = 0,\ \forall\, x \in M\}$.

i. Prove that M is faithful if and only if $\mathrm{Ann}(M) = \{0\}$.

ii. Prove that $\mathrm{Ann}(M)$ is a two-sided ideal of R.

iii. Prove that M is a faithful module as a module for the quotient ring $R/\mathrm{Ann}(M)$.

Solution.

i. M is faithful if and only if the associated representation $\rho_M : R \to \mathrm{End}(M)$ is injective, i.e. the only $a \in R$ such that $aM = 0$ is $a = 0$, that is, if and only if $\mathrm{Ann}(M) = \{0\}$.

ii. Since R is commutative, every ideal is two-sided. Now, $0 \in \mathrm{Ann}(M)$ and $(a - b)x = ax - bx = 0$ for all $a, b \in \mathrm{Ann}(M)$ and all $x \in M$ show that $\mathrm{Ann}(M)$ is an additive subgroup of R. Moreover $(ca)x = c(ax) = 0$ for all $c \in R$.

iii. First, note that M is indeed an $R/\operatorname{Ann}(M)$-module by defining $(a+\operatorname{Ann}(M))x = ax$ for any $a+\operatorname{Ann}(M) \in R/\operatorname{Ann}(M)$ and $x \in M$. In particular, $0 = (a+\operatorname{Ann}(M))M = aM$ shows that $a \in \operatorname{Ann}(M)$, i.e. $a+\operatorname{Ann}(M) = 0_{R/\operatorname{Ann}(M)}$.

Exercise 2.6. Let R be a commutative ring.

- Let M be an R-module. Prove that $\operatorname{Hom}_R(R, M)$ is an R-module isomorphic to M.
- Prove that $\operatorname{End}_R M$ is a unital ring, generally not commutative.

Solution.

- Let $H_M = \operatorname{Hom}_R(R, M)$. Note that any $\varphi \in H_M$ is determined by $\varphi(1)$, since $\varphi(a) = a\varphi(1)$ for all $a \in R$. Any choice of $\varphi(1) \in M$ gives rise to a uniquely defined R-homomorphism. In other words, the map $\eta : H_M \to M$, given by $\eta(\varphi) = \varphi(1)$ is bijective. Moreover, from the previous exercise, we have $\eta(a\varphi) = (a\varphi)(1) = a(\varphi(1)) = a\eta(\varphi)$, for all $a \in R$ and all $\varphi \in H_M$. The assertion follows.
- Composition of R-endomorphisms of M is an R-endomorphism. Composition of maps is associative and distributes over the sum (routine verification): $\varphi\circ(\psi_1+\psi_2) = \varphi\circ\psi_1+\varphi\circ\psi_2$ and $(\psi_1+\psi_2)\circ\varphi = \psi_1\circ\varphi+\psi_2\circ\varphi$, for all $\varphi, \psi_1, \psi_2 \in \operatorname{End}_R(M)$ since addition is defined pointwise. The multiplicative identity is the identity map on M. The composition of maps is not commutative in general, e.g. $M = \mathbb{Z} \oplus \mathbb{Z}$ gives $\operatorname{End}_{\mathbb{Z}}(M) \cong M_2(\mathbb{Z})$, the 2×2 matrices with integer coefficients.

Exercise 2.8. Let R be a commutative ring. Prove that, given any R-homomorphism $\varphi \in \operatorname{Hom}_R(M, N)$, we obtain an exact sequence

$$0 \longrightarrow \ker(\varphi) \xrightarrow{incl} M \xrightarrow{\varphi} N \xrightarrow{\pi} \operatorname{coker}(\varphi) \longrightarrow 0\ .$$

Solution. By construction, $\ker(\varphi) = \operatorname{im}(incl)$, and $\operatorname{im}(\varphi) = \ker(\pi)$ since $\operatorname{coker}(\varphi) = N/\operatorname{im}(\varphi)$ and $\pi : N \to N/\operatorname{im}(\varphi)$ is the quotient map. Moreover, inclusion is injective and π is projective by definition.

Exercise 2.9. Let R be a ring. Prove that a short exact sequence $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ of R-modules splits if and only if B is isomorphic to $A \oplus C$.

Solution. Suppose that $B = A \oplus C$. Our exact sequence is

$$0 \longrightarrow A \xrightarrow{i_A} A \oplus C \xrightarrow{p_C} C \longrightarrow 0\ .$$

Then it is split via the inclusion $i_C : C \to A \oplus C$ into the C summand.

Conversely, suppose that the sequence splits, and let $s : C \to B$ be a section of g, i.e. $gs = \operatorname{Id}_C$. Note that this is equivalent to requiring $sgs = s$, since, by injectivity of s, the equality $s(gs - \operatorname{Id}_C) = 0$ implies $gs = \operatorname{Id}_C$. The injectivity of s also implies that $\operatorname{im}(g) = C \cong \operatorname{im}(s)$, which is a submodule of B. Since the sequence is exact, $\ker(g) = \operatorname{im}(f) \cong A$, and so $B = \ker(g) + \operatorname{im}(s) \cong A + C$. Now observe that $\operatorname{im}(s) \cap \ker(g) = 0$ since $gs = \operatorname{Id}_C$.

Exercise 2.10 (Five Lemma)**.** Let R be a ring. Suppose that we have a commutative diagram of R-modules and R-homomorphisms, of the form

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "a"] & B \arrow[r, "g"] \arrow[d, "b"] & C \arrow[r, "h"] \arrow[d, "c"] & D \arrow[r, "i"] \arrow[d, "d"] & E \arrow[d, "e"] \\ A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r, "h'"] & D' \arrow[r, "i'"] & E' \end{tikzcd},$$

with exact rows. *Commutative* means that all the 'paths' between two modules are equal, e.g. $f'a = bf$.

i. Suppose that b, d are surjective and e injective. Prove that c is surjective.

ii. Suppose that b, d are injective and a surjective. Prove that c is injective.

iii. Suppose that a, b, d, e are isomorphisms. Prove that c is an isomorphism.

Solution. All these are typical *diagram chasing* exercises.

i. Let $x \in C'$. Then $h'(x) \in D' = \operatorname{im}(d)$. Choose $y \in d^{-1}(h'(x))$. We have $ei(y) = i'd(y) = i'h'(x) = 0$. Since e is injective, $y \in \ker(i) = \operatorname{im}(h)$. Choose $z \in h^{-1}(y)$. We have $h'c(z) = dh(z) = d(y) = h'(x)$. So $c(z) - x \in \ker(h') = \operatorname{im}(g')$. Let $u \in (g')^{-1}\big(c(z) - x\big)$. By surjectivity of b, there exists $v \in B$ such that $b(v) = u$, and so $g'b(v) = g'(u) = c(z) = x$, showing that c is surjective.

ii. This is a very similar exercise.

iii. This is a corollary of the previous two assertions.

Exercise 2.14. Adapt the proof of Hilbert's basis theorem to show that $R[[x]]$ is Noetherian if R is Noetherian.

Solution. To modify the proof for $R[[x]]$, we replace ideal formed by the leading coefficients, which we used to show Hilbert's basis theorem in the case of polynomial rings, with the ideal formed by the coefficients of least degree. The rest of the proof is then identical.

Exercise 2.15. Let R be a ring, let $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ be a short exact sequence of R-modules and let M be an R-module.

i. Prove that the sequence

$$0 \longrightarrow \operatorname{Hom}_R(M, A) \xrightarrow{f_*} \operatorname{Hom}_R(M, B) \xrightarrow{g_*} \operatorname{Hom}_R(M, C) \quad \text{is exact,}$$

where $f_*(\varphi) = f\varphi : M \to A \to B$ and similarly for g_*.

ii. Prove that the sequence

$$0 \longrightarrow \operatorname{Hom}_R(C, M) \xrightarrow{g^*} \operatorname{Hom}_R(B, M) \xrightarrow{f^*} \operatorname{Hom}_R(A, M) \quad \text{is exact,}$$

where $g^*(\varphi) = \varphi f : B \to C \to M$ and similarly for f^*.

Solution.

i. By definition, for all $\varphi \in \mathrm{Hom}_R(M, A)$, we have $f_*(\varphi) = f\varphi : \ M \xrightarrow{\varphi} A \xrightarrow{f} B$ is the composition, and similarly for the other induced maps. In particular, the composition $g_* f_*$ is zero.

Let $\varphi \in \mathrm{Hom}_R(M, A)$ such that $\varphi \in \ker(f_*)$. That is $0 = f(\varphi(x))$ for all $x \in M$. By injectivity of f, this holds if and only if $x \in \ker(\varphi)$, for all $x \in M$; that is, $\varphi = 0$. Thus f_* is injective.

Similarly, let $\varphi \in \mathrm{Hom}_R(M, B)$ such that $\varphi \in \ker(g_*)$. That is, $0 = g(\varphi(x))$ for all $x \in M$. Since $\ker(g) = \mathrm{im}(f)$, for all $x \in M$, we can pick $y_x \in A$ such that $\varphi(x) = f(y_x) \in B$, and such a y_x is unique by injectivity of f. Hence the map $\psi : M \to A$, defined by $\psi(x) = y_x$ is well-defined, and it is routine to check that ψ is an R-homomorphism. In other words, $\varphi = f\psi = f_*(\psi) \in \mathrm{im}(f_*)$ as was left to be shown.

ii. By definition, for all $\varphi \in \mathrm{Hom}_R(C, M)$, we have $f^*(\varphi) = \varphi f : B \xrightarrow{f} C \xrightarrow{\varphi} M$ is the precomposition, and similarly for the other induced maps. In particular, the composition $f^* g^*$ is zero.

Note that $C = \mathrm{im}(g)$, and so if $\varphi \in \ker(g^*)$, i.e. $0 = \varphi g : B \to M$, then $\varphi = 0$. Therefore g^* is injective.

Similarly, if $\varphi \in \ker(f^*)$, i.e. $0 = \varphi f : A \to M$, then $\ker(\varphi) \supseteq \mathrm{im}(f) = \ker(g)$. Therefore φ factors through $B/\ker(g) \cong C$: Let $\alpha : C \to B/\ker(g)$ be an R-isomorphism,

$$\begin{tikzcd} B \arrow[r, "\varphi"] \arrow[d, "g"'] & M \\ C \arrow[r, "\alpha"] & B/\ker(g) \arrow[u, "\overline{\varphi}"'] \end{tikzcd}$$

and set $\psi = \overline{\varphi}\alpha$, where $\overline{\varphi}(x + \ker(g)) = \varphi(x)$.

Then $\varphi = \overline{\varphi}\alpha g = \psi g = g^*(\psi)$ by construction, i.e. $\varphi \in \mathrm{im}(g^*)$ for all $\varphi \in \ker(f^*)$.

Exercise 2.18. Let R be a commutative ring. An R-module M is *divisible* if $aM = M$ for all $0 \neq a \in R$. That is, the multiplication by a map $M \to M$ is a surjective R-homomorphism.

i. Prove that $\mathbb{Q}$ is a divisible $\mathbb{Z}$-module (i.e. abelian group).

iv. Prove that an injective R-module is divisible.

Solution.

i. For all $0 \neq a \in \mathbb{Z}$, and for all $x \in \mathbb{Q}$, we have $x = a(\frac{x}{a})$. So $\mathbb{Q} = a\mathbb{Q}$ for all nonzero $a \in \mathbb{Z}$.

ii. We prove a stronger result: *Let R be a PID and let M be an R-module. Then M is injective if and only if M is divisible, i.e. for all $0 \neq a \in R$ and all $x \in M$, there exists $y \in M$ such that $ay = x$.*

Suppose M injective and let $0 \neq a \in R$ and $x \in M$. Define $\alpha_x \in \mathrm{Hom}_R(R, M)$ defined by $\alpha_x(1) = x$, and let $\mu_a \in \mathrm{End}_R(R)$ be the multiplication by a map, i.e. $\mu_a(1) = a$. Since R is an ID, μ_a is injective. Since M is injective, there exists an R-homomorphism $\beta \in \mathrm{Hom}_R(R, M)$ such that the diagram (in R $-$mod)

$$\begin{tikzcd} R \arrow[r, "\mu_a"] \arrow[d, "\alpha_x"'] & R \arrow[dl, "\beta"] \\ M & \end{tikzcd}$$

commutes.

Thus M is divisible. (Note that this implication does not require R to be a PID, but only an ID.)

Conversely, suppose that M is divisible. Let $M \qquad A \underset{f}{\overset{g}{\hookrightarrow}} B$ be a diagram in R $-$mod. We need to construct $h \in \mathrm{Hom}_R(B, M)$ such that $hg = f$.

Let $\mathcal{X} = \{(C, k) \mid A \subseteq C \subseteq B, \ k \in \mathrm{Hom}_R(C, M), \ \mathrm{res}^C_A(k) = f\}$, where $\mathrm{res}^C_A(k)$ denotes the restriction of the R-homomorphism k to A. The relation $(C, k) \leq (C', k') \iff C \subseteq C'$ and

$\mathrm{res}_C^{C'}(k') = k$ endows $\mathcal{X}$ with a partial order. Note that $(A, f) \in \mathcal{X}$, and that $\mathcal{X}$ satisfies the hypothesis of Zorn's lemma: if $(C_1, k_1) \leq (C_2, k_2) \leq \ldots$ is a chain in $\mathcal{X}$, then the pair $\big(\cup_i C_i\ ,\ \cup_i k_i\big) \in \mathcal{X}$, where $\cup_i k_i(x) = k_j(x)$ for any j such that $x \in C_j$ is a well-defined R-homomorphism.

Hence, by Zorn's lemma, $\mathcal{X}$ contains a maximal element (C, k). It suffices to show that $C = B$. Suppose $C \subsetneq B$, and pick $x \in B \setminus C$. Let $I = \{a \in R \mid ax \in C\}$. Then I is an idel of R, and since R is a PID, there exists $d \in R$ such that $I = (d)$.

If $d = 0$, choose any element $y \in M$. If $d \neq 0$, then, since M is divisible, there exists $y_a \in M$ such that $k(ax) = ay_a$ for all $a \in R$.

Hence define $\hat{k} : (C + Rx) \to M$ by $\hat{(k)}(u + ax) = k(u) + ay_a$ for all $u \in C$ and all $a \in R$.

Note that $\hat{k}$ is well-defined: If $ax \in C$, then $\hat{k}(ax) = ay_a$ (whether $d = 0$ or $d \neq 0$). Now $ax \in C$ implies that $a \in I = (d)$ by definition of I, i.e there exists $\lambda \in R$ such that $a = \lambda d$, and it follows that $ax = \lambda dx$, implying that $\hat{k}(ax) = \lambda k(dx) = \lambda dy = ay$.

But this is impossible, by maximality of (C, k). Therefore, we must have $C = B$, showing that there exists $h : B \to M$ such that $f = hg$.

Exercise 2.20. Let R be a PID and let M be a nonzero finitely generated torsionfree R-module. Prove that M is free. (Hint: proceed by induction on the number of generators of M.)

Solution. See Corollary 29.28 in Isaacs, *Algebra - A graduate course*, Graduate Studies in Mathematics 100, American Mathematical Society, 2009.

Note that this question is not examinable, but is a very useful result.
