Math 5591H **Solutions to some problems from sections 10.1 and 10.2**

Let R be a ring and M be a left R-module.

10.1.3. *Assume that $1 \in R$ and let $au = 0$ for some $a \in R$ and some $u \in M$ with $u \neq 0$. Prove that a does not have a left inverse.*

Solution. If $ba = 1$ then $u = bau = 0$.

Another solution. $\mathrm{Ann}(u)$ is a proper left ideal, so it cannot contain right units of R.

10.1.5. *For a left ideal I of R define $IM = \{\sum_{i=1}^{k} a_i u_i : a_i \in I,\ u_i \in M\}$. Prove that IM is a submodule of M.*

Solution. If $u, v \in IM$, $u = \sum_{i=1}^{k} a_i u_i$ and $v = \sum_{j=1}^{l} a_i v_j$ with $a_i, b_j \in I$, $u_i, v_j \in M$ for all i, j, then $u + v = a_1u_1 + \cdots + a_ku_k + b_1v_1 + \cdots + b_lv_l \in IM$, and also $au = (aa_1)u_1 + \cdots + (aa_k)u_k \in IM$ for any $a \in \mathbb{R}$ since $aa_1, \ldots, aa_k \in I$.

10.1.7. *Let $N_1 \subseteq N_2 \subseteq \cdots$ be an ascending chain of submodules of M. Prove that $\bigcup_{i=1}^{\infty} N_i$ is a submodule of M.*

Solution. Let $u, v \in \bigcup_{i=1}^{\infty} N_i$; let $u \in N_i$ and $v \in N_j$. W.l.o.g., assume that $j \geq i$. Then $u \in N_j$, so $u + v \in N_j$, so $u + v \in \bigcup_{i=1}^{\infty} N_i$. Also for any $a \in R$, $au \in N_i$, so $au \in \bigcup_{i=1}^{\infty} N_i$.

Cf. **10.1.8.** *Let M be a (left) R-module, and let $\mathrm{Tor}(M)$ be the set of torsion elements of M, $\mathrm{Tor}(M) = \{u \in M : au = 0$ for some nonzero $a \in R\}$.*

(a) *If R is an integral domain, prove that $\mathrm{Tor}(M)$ is a submodule of M.*

Solution. Let $u, v \in \mathrm{Tor}(M)$, that is, $au = 0$ and $bv = 0$ for some nonzero $a, b \in R$. Then $ab(u - v) = 0$ and $ab \neq 0$ since R is an integral domain, and for any $c \in R$, $a(cu) = c(au) = 0$ since R is commutative. Hence, $\mathrm{Tor}(M)$ is a subgroup and a submodule.

(b) *If R is an integral domain, prove that $M/\mathrm{Tor}(M)$ is torsion-free (that is, $\mathrm{Tor}\big(M/\mathrm{Tor}(M)\big) = 0$).*

Solution. Assume that $a\overline{u} = 0$ in $M/\mathrm{Tor}(M)$ for some $u \in R$ and nonzero $a \in R$, where $\overline{u} = u + \mathrm{Tor}(M) \in M/\mathrm{Tor}(M)$. This means that $au \in \mathrm{Tor}(M)$; hence there exists a nonzero $b \in R$ such that $bau = 0$. But $ab \neq 0$ since R is an integral domain, so $u \in \mathrm{Tor}(M)$, and so $\overline{u} = 0$ in $M/\mathrm{Tor}(M)$.

(c) *Give an example of a ring R and an R-module M such that $\mathrm{Tor}(M)$ is not a module.*

Solution. Let $M = R = \mathbb{Z}_6$. Then $\mathrm{Tor}(M) = \{0, 2, 3, 4\}$ (indeed, $3 \cdot 2 = 0$, $2 \cdot 3 = 0$, $3 \cdot 4 = 0$, and $a \cdot 1, a \cdot 5 \neq 0$ for all nonzero $a \in R$), and don't form a submodule of M.

Another solution. In this example, R has no zero divisors, but is noncommutative. Let $R = \mathbb{R}\langle x, y\rangle$, the ring of (real) polynomials in non-commuting(!) variables x and y (that is, the (semi)group ring over $\mathbb{R}$ of the free semigroup generated by x and y, $\{1, x, y, x^2, xy, yx, y^2, \ldots\}$). Let $I = Rx$ and $M = R/I$; then for $p(x, y) \in R$, $\overline{p(x, y)} = 0$ in M iff all the monomials of $p(x, y)$ end with an x. Then $\overline{1} \in \mathrm{Tor}(M)$ since $x\overline{1} = \overline{x} = 0$ in M, but $y\overline{1} = \overline{y} \notin \mathrm{Tor}(M)$ since for any nonzero $p(x, y) \in R$, all the monomials of $p(x, y)y$ end with a y. So, $\mathrm{Tor}(M)$ is not a module.

(d) *If R has zero divisors and $M \neq 0$, prove that $\mathrm{Tor}(M) \neq 0$.*

Solution. Let a and b be nonzero elements of R such that $ab = 0$. Let u be any nonzero element of M. Then if $bu = 0$, then u is a nonzero torsion element of M. And if $bu \neq 0$, then $a(bu) = (ab)u = 0$, so bu is a nonzero torsion element of M.

10.1.9. *If S is a subset of M, prove that $\mathrm{Ann}(S) = \{a \in R : aS = 0\}$ is a left ideal in R. If N is a submodule of M, prove that $\mathrm{Ann}(N)$ is a two-sided ideal in R.*

Solution. If $a, b \in \mathrm{Ann}(S)$, then for any $u \in S$, $(a + b)u = au + bu = 0$, so $a + b \in \mathrm{Ann}(S)$. Also, if $a \in \mathrm{Ann}(N)$, then for any $c \in R$, for every $u \in S$ we have $(ca)u = c(au) = 0$. Hence, $\mathrm{Ann}(S)$ is a left ideal in R.

If N ia submodule of M, then for any $a \in \mathrm{Ann}(N)$ and any $c \in R$ for every $u \in N$ we have $cu \in N$, so $(ac)(u) = a(cu) = 0$, so $ac \in \mathrm{Ann}(N)$ as well. Hence, $\mathrm{Ann}(N)$ is a two-sided ideal in R.

10.1.10. *If I is a right ideal in R, prove that* $\mathrm{Ann}(I) = \{u \in M : Iu = 0\}$ *is a submodule of M.*

Solution. If $u, v \in \mathrm{Ann}(I)$, then for any $a \in I$, $a(u+v) = au + av = 0$, so $u + v \in \mathrm{Ann}(I)$. Also, if $u \in \mathrm{Ann}(I)$, then for any $b \in R$, for any $a \in I$, $a(bu) = (ab)u = 0$ since $ab \in I$; so, $bu \in \mathrm{Ann}(I)$. Hence, $\mathrm{Ann}(I)$ is a submodule of M.

10.1.11. *Let M be the abelian group (i.e., a $\mathbb{Z}$-module) $\mathbb{Z}_{24} \times \mathbb{Z}_{15} \times \mathbb{Z}_{50}$.*

(a) *Find the annihilator of M in $\mathbb{Z}$.*

Solution. $n \in \mathbb{Z}$ annihilates M iff n is divisible by 24, 15, and 50. So, $\mathrm{Ann}(M) = (n)$ where $n = \mathrm{lcd}\{24, 15, 50\} = 600$.

(b) *Let $I = 2\mathbb{Z}$. Describe the annihilator of I in M as a direct product of cyclic groups.*

Solution. $u = (u_1, u_2, u_3)$ annihilates 2 (and so $2\mathbb{Z}$) iff $2u_1 = 0 \bmod 24$, so $u_1 = 0$ or 12; $2u_2 = 0 \bmod 15$, so $u_2 = 0$; and $2u_3 = 0 \bmod 50$, so $u_3 = 0$ or 25. So, $\mathrm{Ann}(2\mathbb{Z}) = \{0, 12\} \times \{0\} \times \{0, 25\} \cong \mathbb{Z}_2^2$.

10.1.13. *Let I be a right ideal of R. Let M' be the subset of elements a of M that are annihilated by some power, I^k of the ideal I. Prove that M' is a submodule of M.*

Solution. We have $M' = M_1 \cup M_2 \cup \cdots$, where $M_k = \mathrm{Ann}(I^k)$, $k \in \mathbb{N}$. For any k, since $I^k \supseteq I^{k+1}$, we have $M_k \subseteq M_{k+1}$, so $M_1 \subseteq M_2 \subseteq \cdots$. Hence, M' is a submodule of M.

10.1.15. *If M is a finite abelian group then M is naturally a $\mathbb{Z}$-module. Can this action be extended to make M into a $\mathbb{Q}$-module?*

Solution. No, unless $M = 0$: any nonzero $\mathbb{Q}$-module ($\mathbb{Q}$-vector space) is infinite.

Or: Take any nonzero $u \in M$; the mapping $\mathbb{Q} \longrightarrow M$, $a \mapsto au$, is injective, so $|M| \geq |\mathbb{Q}|$ and M is infinite.

10.1.18-20. *Let $F = \mathbb{R}$. Let $V = \mathbb{R}^2$ and let T be a linear transformation $V \longrightarrow V$; then V is an $F[x]$-module by $xu = T(u)$, $u \in V$. Find the $F[x]$-submodules of V if*

(a) *T is rotation clockwise about the origin by $\pi/2$.*

(b) *T is the projection onto the y-axis.*

(c) *T is rotation clockwise about the origin by π radians.*

Solution. $F[x]$-submodules of V are T-invariant subspaces of V. In (a), these are 0 and V only; in (b), these are 0, V, $\mathbb{R} \times 0$ and $0 \times \mathbb{R}$ only; in (c), these are all subspaces of V.

10.2.4. *Let A be any $\mathbb{Z}$-module, let u be any element of M and let $n \in \mathbb{N}$. Prove that the map $\varphi_u \colon \mathbb{Z}_n \longrightarrow A$ given by $\varphi_u(\bar{k}) = ka$, $k \in \mathbb{Z}$, is a well defined $\mathbb{Z}$-module homomorphism iff $nu = 0$. Prove that* $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, A) \cong A_n$ *where $A_n = \{a \in A : na = 0\}$ (so $A_n = \mathrm{Ann}(n)$).*

Solution. Let's consider the general situation: let $\varphi \colon M \longrightarrow N$ be a module homomorphism and let K be a submodule of N. Can φ be factorized to M/K, that is, is there a homomorphism $\widetilde{\varphi} \colon M/K \longrightarrow N$ such that $\varphi = \widetilde{\varphi} \circ \pi$ where π is the natural homomorphism $M \longrightarrow M/K$? For $\widetilde{\varphi}$ to exist it is necessary and sufficient that φ is constant on the cosets of K in M, in which case we put $\widetilde{\varphi}(\overline{u}) = \varphi(u)$ for any $u \in M$, $\overline{u} = u + K$. And this is so iff $K \subseteq \ker \varphi$.

Define homomorphism $\psi_u \colon \mathbb{Z} \longrightarrow A$ by $\psi_u(k) = ku$. And we know that it can be factorized to the homomorphism $\varphi_u \colon \mathbb{Z}_n \longrightarrow A$ iff $(n) \subseteq \ker \psi_u = \mathrm{Ann}(u)$, that is, iff $nu = 0$.

Now, all homomorphisms $\mathbb{Z} \longrightarrow A$ have form $\psi_u(k) = ku$, $u \in A$. (Indeed, if $\psi \colon \mathbb{Z} \longrightarrow A$ is a homomorphism, put $u = \varphi(1)$, then $\psi(k) = ku$ for all $k \in \mathbb{Z}$, so $\psi = \psi_u$.) So, we have a bijection $A \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A)$, $u \mapsto \psi_u$. This bijection is an isomorphism of $\mathbb{Z}$-modules (=abelian groups), since $\varphi_{u+v} = \psi_u + \psi_v$ and $\psi_{mu} = m\psi_u$ for any $u, v \in A$ and $m \in \mathbb{Z}$. So, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A) \cong A$ as $\mathbb{Z}$-modules (as groups).

Now, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, A)$ is (isomorphic to) the submodule of $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A)$ that consists of homomorphisms ψ_u such that $nu = 0$, $\varphi_a \leftrightarrow \psi_a$, which is isomorphic to the submodule $\{u \in M : nu = 0\} = \mathrm{Ann}(n)$.

(All this, actually, applies to any commutative unital ring R (instead of $\mathbb{Z}$) and an R-module M: $\mathrm{Hom}_R(R, M) \cong M$ and for any ideal I of R, $\mathrm{Hom}_R(R/I, M) = \mathrm{Ann}(I) \subseteq M$.)

10.2.6. *Prove that* $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_m) \cong \mathbb{Z}_d$, *where $d = \gcd(n, m)$.*

Solution. The mapping $\Phi: \varphi \mapsto \varphi(1) \in \mathbb{Z}_m$ is a homomorphism of abelian groups (= of $\mathbb{Z}$-modules) $\Phi: \mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}_m) \longrightarrow \mathbb{Z}_m$. Since $\mathbb{Z}_n$ is generated by 1, any homomorphism $\varphi \in \mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}_m)$ is uniquely defined by $\varphi(1)$, thus Φ is injective. Since $0 = \varphi(n) = n\varphi(1)$ in $\mathbb{Z}_m$, the order of the element $\varphi(1) \in \mathbb{Z}_m$ must divide n, and conversely, if $k \in \mathbb{Z}_m$ is such that $nk = 0$, then the mapping $x \mapsto kx$ is a homomorphism $\mathbb{Z}_n \longrightarrow \mathbb{Z}_m$. (Since in this case, $n\mathbb{Z}$ is contained in the kernel of the homomorphism $\mathbb{Z} \longrightarrow \mathbb{Z}_m$, $x \mapsto kx$.) Thus, Φ maps $\mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}_m)$ onto the subgroup of elements of $\mathbb{Z}_m$ of order dividing n, which is $(m/d)\mathbb{Z}_m$ and is isomorphic to $\mathbb{Z}_d$.

10.2.7. *Let $z \in Z(R)$, the center of R. Prove that the map $u \mapsto zu$ is an R-module homomorphism from M to itself. Show that for a commutative ring R the map from R to $\mathrm{End}_R(M)$ given by $a \mapsto a\,\mathrm{Id}_M$ is a ring homomorphism (where Id_M is the identity endomorphism of M).*

Solution. If $z \in Z(R)$, put $\varphi_z(u) = zu$, $u \in M$, or $\varphi_z = z\,\mathrm{Id}_M$; then $\varphi_z(u + v) = z(u + v) = zu + zv = \varphi_z(v) + \varphi_z(v)$ and $\varphi_z(au) = zau = azu = c\varphi_z(u)$ for any $u, v \in M$ and $a \in \mathbb{R}$, so φ_z is an endomorphism of M.

Let R be commutative, so that $Z(R) = R$. Then we have the mapping $R \longrightarrow \mathrm{End}_R(M)$, $a \mapsto \varphi_a$. This mapping is a ring homomorphism, since $\varphi_{a+b}(u) = (a + b)u = au + bu = \varphi_a(u) + \varphi_b(u)$, $\varphi_{ab}(u) = (ab)u = a(bu) = \varphi_a(\varphi_b(u))$, $u \in M$, so $\varphi_{a+b} = \varphi_a + \varphi_b$ and $\varphi_{ab} = \varphi_a \circ \varphi_b$ for all $a, b \in R$.

10.2.8. *Let $\varphi: M \longrightarrow N$ be an R-module homomorphism. Prove that $\varphi(\mathrm{Tor}(M)) \subseteq \mathrm{Tor}(N)$.*

Solution. If $u \in \mathrm{Tor}(M)$, $au = 0$ for some $a \neq 0$, then $a\varphi(u) = \varphi(au) = 0$, so $\varphi(u) \in \mathrm{Tor}(N)$.

10.2.10. *Let R be a unital commutative ring. Prove that $\mathrm{End}_R(R)$ and R are isomorphic as rings.*

Solution. Every $a \in R$ defines an endomorphism φ_a of R by $\varphi(b) = ab$, $b \in R$. And any endomorphism φ of R has this form: let $a = \varphi(1)$, then for any $b \in R$, $\varphi(b) = b\varphi(1) = ba = ab$, so $\varphi = \varphi(a)$. We therefore have a bijection $R \longrightarrow \mathrm{End}_R(R)$, $a \mapsto \varphi_a$. This bijection is a homomorphism: for any $a, c \in R$, $\varphi_{a+c}(b) = (a + c)b = ab + cb = \varphi_a(b) + \varphi_c(b)$ for all $b \in R$, so $\varphi_{a+c} = \varphi_a + \varphi_c$. Also, $\varphi_{ac}(b) = acb = \varphi_a(\varphi_c(b))$ for all $b \in R$, so $\varphi_{ac} = \varphi_a \circ \varphi_c$. Hence, the mapping $a \mapsto \varphi_a$ is an isomorphism.

10.2.11. *Let $A_1, A_2, \ldots, A_n$ be R-modules and let B_i be a submodule of A_i for each i. Prove that $(A_1 \times \cdots \times A_n)/(B_1 \times \cdots \times B_n) \cong (A_1/B_1) \times \cdots \times (A_n/B_n)$.*

Solution. Define the homomorphism $\varphi: A_1 \times \cdots \times A_n \longrightarrow (A_1/B_1) \times \cdots \times (A_n/B_n)$ by $\varphi(u_1, \ldots, u_n) = \big(u_1 \bmod B_1, \ldots, u_n \bmod B_n\big)$. φ is, clearly, surjective, and $\ker(\varphi) = B_1 \times \cdots \times B_n$. By the 1-st isomorphism theorem, $(A_1 \times \cdots \times A_n)/(B_1 \times \cdots \times B_n) \cong (A_1/B_1) \times \cdots \times (A_n/B_n)$.

10.2.12. *Let I be a left ideal of R and let n be a positive integer. Prove that $R^n/(IR^n) \cong \big(R/(IR)\big)^n$.*

Solution. Notice that $IR^n = (IR)^n$: indeed, both modules are generated by elements $(0, \ldots, 0, ra, 0, \ldots, 0)$, where $r \in I$ and $a \in R$. So, the assertion follows from 10.2.11.

10.2.13. *Let I be a nilpotent ideal in a commutative ring R, that is, $I^n = 0$ for some n; let M and N be R-modules and let $\varphi: M \longrightarrow N$ be a homomorphism. Show that if the induced homomorphism $\bar{\varphi}: M/IM \longrightarrow N/IN$ is surjective, then φ is surjective.*

Solution. First, the homomorphism $\bar{\varphi}: M/IM \longrightarrow N/IN$ is well defined since $\varphi(IM) \subseteq IN$.

Let's show that the induced homomorphism $IM \longrightarrow IN/I^2N$ (and so, $IM/I^2M \longrightarrow IN/I^2N$) is surjective. Indeed, the module IN is generated by elements of the form av with $a \in I$, $v \in N$. For every $v \in N$ there exist $u \in M$ and $w \in IN$ such that $\varphi(u) = v + w$. Then for any $a \in I$, $\varphi(au) = av + aw$ with $aw \in I^2N$. So, av is in the image of the induced homomorphism $IM \longrightarrow IN/I^2N$, and so, this homomorphism is surjective.

We have $I^nM = 0$; let k be the minimal integer such that $I^kM = 0$, and let's use induction on k. We have $I^{k-1}(IM) = 0$, so by induction hypothesis applied to the homomorphism $\varphi|_{IM}: IM \longrightarrow IN$, we have $\varphi(IM) = IN$. We now have the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & IM & \longrightarrow & M & \longrightarrow & M/IM & \longrightarrow & 0 \\ & & \varphi|_{IM}\downarrow & & \varphi\downarrow & & \bar{\varphi}\downarrow & & \\ 0 & \longrightarrow & IN & \longrightarrow & N & \longrightarrow & N/IN & \longrightarrow & 0 \end{array}$$

with exact rows, and with $\varphi|_{IM}$, $\bar{\varphi}$ being surjective. By the short five lemma, φ is also surjective.