Do the following exercises from Chapter 3 of the text (Pages 174–181): 8, 9, 17, 29, 43, 47

8. Show that $\mathbb{Q}$ is a torsion-free $\mathbb{Z}$-module that is not free.

   ▶ **Solution.** $\mathbb{Q}$ is torsion free as a $\mathbb{Z}$ module since $\mathbb{Q}$ is a field that contains $\mathbb{Z}$ as a submodule. Specifically, if $m \neq 0 \in \mathbb{Z}$ and $r \in \mathbb{Q}$ with $mr = 0$, then $m \neq 0$ as an element of $\mathbb{Q}$ and $r = (1/m)(mr) = 0$. Thus $\mathbb{Q}$ is torsion-free as a $\mathbb{Z}$-module.

   To see that $\mathbb{Q}$ is not free as a $\mathbb{Z}$-module, simply note that if $S \subseteq \mathbb{Q}$ is any subset consisting of more than one element, then S is *not* $\mathbb{Z}$-linearly independent. To see this, suppose that r/s and t/u are two distinct elements of S. Then

   $$(st)\frac{r}{s} - (ur)\frac{t}{u} = 0$$

   is a nontrivial $\mathbb{Z}$-linear dependence relation between r/s and t/u, so S is not $\mathbb{Z}$-linearly independent if it contains at least 2 elements. If $S = \{r/s\}$ is a subset of $\mathbb{Q}$ containing exactly one element, then S does not generate $\mathbb{Q}$ as a $\mathbb{Z}$-module. To see this, observe that $1/2s$ cannot be written as an integer multiple of r/s, since, if this were possible then we would have $1/2s = m(r/s)$ for some $m \in \mathbb{Z}$ which would give the equation in integers $1 = 2mr$, which is not possible. ◀

9. (a) Let R be an integral domain, let M be a torsion R-module, and let N be a torsion-free R-module. Show that $\mathrm{Hom}_R(M, N) = \langle 0 \rangle$.

   ▶ **Solution.** Let $f \in \mathrm{Hom}_R(M, N)$ and let $m \in M$. Since M is a torsion module, there is an $r \neq 0 \in R$ with $rm = 0$. Then $0 = f(0) = f(rm) = rf(m)$. Since $r \neq 0$ and N is torsion-free, this implies that $f(m) = 0$. Since $m \in M$ is arbitrary, this gives $f = 0$, as required. ◀

   (b) If $n = km$, then show that $\mathrm{Hom}_{\mathbb{Z}_n}(\mathbb{Z}_m, \mathbb{Z}_n) \cong \mathbb{Z}_m$.

   ▶ **Solution.** Define a map $\varphi : \mathrm{Hom}_{\mathbb{Z}_n}(\mathbb{Z}_m, \mathbb{Z}_n) \to \mathbb{Z}_n$ by $\varphi(f) = f(1)$. This is a $\mathbb{Z}_n$-module homomorphism from the definition of sum and scalar multiplication of functions. If $f(1) = 0$ then $f(r) = rf(1) = 0$ for all $r \in \mathbb{Z}_m$ so $\mathrm{Ker}(\varphi) = \langle 0 \rangle$. If $t \in \mathbb{Z}_n$ is in the image of φ, then $t = f(1)$ for some $f \in \mathrm{Hom}_{\mathbb{Z}_n}(\mathbb{Z}_m, \mathbb{Z}_n)$. Then $mt = mf(1) = f(m) = f(0) = 0$, so the order of t divides m. Conversely, any element of $\mathbb{Z}_n$ whose order divides m is $f(1)$ for some $f \in \mathrm{Hom}_{\mathbb{Z}_n}(\mathbb{Z}_m, \mathbb{Z}_n)$. Thus, the image of φ consists of all elements of $\mathbb{Z}_n$ whose order divides m, i.e., $\mathrm{Im}(\varphi) = \langle k \rangle \cong \mathbb{Z}_m$. ◀

17. Give examples of short exact sequences of R-modules

   $$0 \longrightarrow M_1 \xrightarrow{\phi} M \xrightarrow{\phi'} M_2 \longrightarrow 0$$

   and

   $$0 \longrightarrow N_1 \xrightarrow{\psi} N \xrightarrow{\psi'} N_2 \longrightarrow 0$$

   such that

(a) $M_1 \cong N_1$, $M \cong N$, $M_2 \ncong N_2$;

► **Solution.** For $n \in \mathbb{N}$, consider the short exact sequence

$$(*_n) \qquad 0 \longrightarrow \mathbb{Z} \xrightarrow{\phi_n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_n \longrightarrow 0$$

where $\phi_n(x) = nx$ and π is the standard projection map. Then choosing any two natural numbers $n \neq m$ will give two short exact sequences $(*_n)$ and $(*_m)$ with the first two terms equal in each sequence, the third terms $\mathbb{Z}_n \ncong \mathbb{Z}_m$. ◄

(b) $M_1 \cong N_1$, $M \ncong N$, $M_2 \cong N_2$;

► **Solution.** For this part, you can use the two short exact sequences from Example 3.8, Page 122:

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{\phi} \mathbb{Z}_{pq} \xrightarrow{\psi} \mathbb{Z}_p \longrightarrow 0$$

and

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{f} \mathbb{Z}_{p^2} \xrightarrow{g} \mathbb{Z}_p \longrightarrow 0,$$

where p and q are distinct primes, $\phi(m) = qm \in \mathbb{Z}_{pq}$, $f(m) = pm \in \mathbb{Z}_{p^2}$ and ψ and g are the canonical projection maps. ◄

(c) $M_1 \ncong N_1$, $M \cong N$, $M_2 \cong N_2$.

► **Solution.** Let M be the $\mathbb{Z}$-module consisting of sequences of elements from the field $\mathbb{Z}_2$. That is,

$$M = \{(a_0, a_1, a_2, \ldots) : a_j \in \mathbb{Z}_2\}.$$

For each natural number $n \in \mathbb{N}$ define a map $\psi_n : M \to M$ by

$$\psi_n(a_0, a_1, a_2, \ldots) = (a_n, a_{n+1}, a_{n+2}, \ldots).$$

It is clear that ψ_n is a $\mathbb{Z}$-module homomorphism and that it is surjective. Moreover, if $n \geq 1$,

$$\mathrm{Ker}(\psi_n) = \{(a_0, a_1, \ldots, a_{n-1}, 0, \ldots) : a_j \in \mathbb{Z}_2\} \cong \mathbb{Z}_2^n.$$

Thus, for each $n \in \mathbb{N}$ there is a short exact sequence

$$(*_n) \qquad 0 \longrightarrow \mathbb{Z}_2^n \xrightarrow{\phi_n} M \xrightarrow{\psi_n} M \longrightarrow 0$$

where

$$\phi_n(a_0, \ldots, a_{n-1}) = (a_0, a_1, \ldots, a_{n-1}, 0, \ldots).$$

Since $\mathbb{Z}_2^n \ncong \mathbb{Z}_2^m$ if $m \neq n$, the short exact sequences $(*_n)$ and $(*_m)$ for $m \neq n$ give the required example. ◄

29. Let $R = \mathbb{Z}_{30}$ and let $A \in M_{2,3}(R)$ be the matrix

$$A = \begin{bmatrix} 1 & 1 & -1 \\ 0 & 2 & 3 \end{bmatrix}.$$

Show that the two rows of A are linearly independent over R, but that any two of the three columns are linearly dependent over R.

▶ **Solution.** As far as the rows are concerned, suppose there is an R-linear dependence relation

$$r\begin{bmatrix} 1 & 1 & -1 \end{bmatrix} + s\begin{bmatrix} 0 & 2 & 3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}.$$

This implies that $r = 0$ which then says that $2s = 0$ and $3s = 0$ so that $s = 3s - 2s = 0$. Thus the rows are linearly independent over R. As for the columns, note that

$$15\begin{bmatrix} 1 \\ 0 \end{bmatrix} + 15\begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}; \quad 10\begin{bmatrix} 1 \\ 0 \end{bmatrix} + 10\begin{bmatrix} -1 \\ 3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}; \text{ and } 6\begin{bmatrix} 1 \\ 2 \end{bmatrix} + 6\begin{bmatrix} -1 \\ 3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Thus, any two of the three columns are R-linearly dependent. ◀

43. Suppose R is a PID and $M = R\langle x\rangle$ is a cyclic R-module with $\operatorname{Ann}(x) = \langle a\rangle \neq \langle 0\rangle$. Show that if N is a submodule of M, then N is cylic with $\operatorname{Ann} N = \langle b\rangle$ where b is a divisor of a. Conversely, show that M has a unique submodule N with annihilator $\langle b\rangle$ for each divisor b of a.

▶ **Solution.** Define an R-module homomorphism $\varphi : R \to M$ by $\varphi(r) = rx$. Since M is cyclic with generator x, φ is surjective and $\operatorname{Ker}(\varphi) = \operatorname{Ann}(x) = \langle a\rangle$. By the first isomorphism theorem for R-modules, there is an isomorphism $\overline{\varphi} : R/\langle a\rangle \to M$, and by the correspondence theorem, φ provides a one-to-one correspondence between the submodules of M and the submodules of R containing $\langle a\rangle$, with the submodule N corresponding to $\varphi^{-1}(N)$. But R is a PID so R-submodules of R are just principal ideals. Thus $\varphi^{-1}(N) = \langle c\rangle \supseteq \langle a\rangle$, so that $N = \varphi(\langle c\rangle) = \{r(cx) : r \in R\}$. Then the annihilator of N is

$$\operatorname{Ann}(N) = \{r \in R : r(cx) = 0\} = \{r \in R : a|rc\} = \langle \frac{a}{c}\rangle.$$

Thus, the annihilator of N is generated by the divisor $b = a/c$ of a. Conversely, if b is any divisor of a, then the submodule $N = \langle (a/b)x\rangle \subset M$ is a submodule with $\operatorname{Ann}(N) = \langle b\rangle$. Therefore, the pairing $b \longleftrightarrow \langle (a/b)x\rangle$ sets up a one-to-one correspondence between divisors of a and submodules of N. ◀

47. Let $u = (a, b) \in \mathbb{Z}^2$.

(a) Show that there is a basis of $\mathbb{Z}^2$ containing u if and only if a and b are relatively prime.

► **Solution.** Suppose that $v = (c, d)$ and that the two vectors u and v form a basis of $\mathbb{Z}^2$. Then there are integers k, l, m and n such that

$$\begin{aligned} ku + lv &= (1, 0) \\ mu + nv &= (0, 1), \end{aligned}$$

which gives the matrix equation

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} \begin{bmatrix} k & m \\ l & n \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Taking determinants then gives $(ad - bc)(kn - ml) = 1$. Since this is an equation in integers, it follows that $ad - bc = \pm 1$ so that a and b are relatively prime.

Conversely, if a and b are relatively prime, then we can write $ra + sb = 1$ and we claim that $u = (a, b)$ and $v = (-s, r)$ form a basis of $\mathbb{Z}^2$. Consider the linear equation

$$xu + yv = (\alpha, \beta)$$

in integers. This is equivalent to the matrix equation

$$\begin{bmatrix} a & -s \\ b & r \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}.$$

Multiplying this equation on the left by the matrix $\begin{bmatrix} r & s \\ -b & a \end{bmatrix}$ gives

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} r & s \\ -b & a \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} r\alpha + s\beta \\ -b\alpha + a\beta \end{bmatrix}.$$

This equation shows that u and v is a linearly independent generating set for $\mathbb{Z}^2$, i.e., a basis. ◄

(b) Suppose that $u = (5, 12)$. Find a $v \in \mathbb{Z}^2$ such that $\{u, u\}$ is a basis of $\mathbb{Z}^2$.

► **Solution.** Since $5 \cdot 5 + (-2) \cdot 12 = 1$, the calculation done in part (a) shows that we can take $v = (2, 5)$. ◄