We can rewrite this as

$$[e_1, \dots, e_s] = [f_1, \dots, f_n]A, \tag{M.4.5}$$

where A denotes the n–by–s matrix $A = (a_{i,j})$. According to Proposition M.4.7, there exist invertible matrices $P \in \mathrm{Mat}_n(R)$ and $Q \in \mathrm{Mat}_s(R)$ such that $A' = PAQ$ is diagonal,

$$A' = PAQ = \mathrm{diag}(d_1, d_2, \dots, d_s).$$

We will see below that all the d_j are necessarily nonzero. Again, according to Proposition M.4.7, P and Q can be chosen so that d_i divides d_j whenever $i \le j$. We rewrite (M.4.5) as

$$[e_1, \dots, e_s]Q = [f_1, \dots, f_n]P^{-1}A'. \tag{M.4.6}$$

According to Lemma M.4.11, if we define $\{v_1, \dots, v_n\}$ by

$$[v_1, \dots, v_n] = [f_1, \dots, f_n]P^{-1}$$

and $\{w_1, \dots, w_s\}$ by

$$[w_1, \dots, w_s] = [e_1, \dots, e_s]Q,$$

then $\{v_1, \dots, v_n\}$ is a basis of F and $\{w_1, \dots, w_s\}$ is a basis of N. By Equation (M.4.6), we have

$$[w_1, \dots, w_s] = [v_1, \dots, v_n]A' = [d_1v_1, \dots, d_sv_s].$$

In particular, d_j is nonzero for all j, since $\{d_1v_1, \dots, d_sv_s\}$ is a basis of N. ■

Exercises M.4

M.4.1. Let R be a commutative ring with identity element and let M be a module over R.

(a) Let A and B be matrices over R of size n–by–s and s–by–t respectively. Show that for $[v_1, \dots, v_n] \in M^n$,

$$[v_1, \dots, v_n](AB) = ([v_1, \dots, v_n]A)B.$$

(b) Show that if $\{v_1, \dots, v_n\}$ is linearly independent subset of M, and $[v_1, \dots, v_n]A = 0$, then $A = 0$.

M.4.2. Prove Lemma M.4.8

M.4.3. Let R denote the set of infinite–by–infinite, row– and column–finite matrices with complex entries. That is, a matrix is in R if, and only if, each row and each column of the matrix has only finitely many non–zero entries. Show that R is a non-commutative ring with identity, and that $R \cong R \oplus R$ as R–modules.

In the remaining exercises, R denotes a principal ideal domain.

M.4.4. Let M be a a free module of rank n over R. Let N be a submodule of M. Suppose we know that N is finitely generated (but not that N is free). Adapt the proof of Theorem M.4.12 to show that N is free.

M.4.5. Let V and W be free modules over R with ordered bases $(v_1, v_2, \dots, v_n)$ and $(w_1, w_2, \dots, w_m)$. Let $\varphi : V \to W$ be a module homomorphism. Let $A = (a_{i,j})$ be the m–by–n matrix whose j^{th} column is the co-ordinate vector of $\varphi(v_j)$ with respect to the ordered basis $(w_1, w_2, \dots, w_m)$,

$$\varphi(v_j) = \sum_i a_{i,j} w_j.$$

Show that for any element $\sum_j x_j v_j$ of M,

$$\varphi(\sum_j x_j v_j) = [w_1, \dots, w_m]\, A \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

M.4.6. Retain the notation of the previous exercise. By Proposition M.4.7, there exist invertible matrices $P \in \mathrm{Mat}_m(R)$ and $Q \in \mathrm{Mat}_n(R)$ such that $A' = PAQ$ is diagonal,

$$A' = PAQ = \mathrm{diag}(d_1, d_2, \dots, d_s, 0, \dots, 0),$$

where $s \le \min\{m, n\}$. Show that there is a basis $\{w_1', \dots, w_m'\}$ of W such that $\{d_1 w_1', \dots, d_s w_s'\}$ is a basis of range(φ).

M.4.7. Set $A = \begin{bmatrix} 2 & 5 & -1 & 2 \\ -2 & -16 & -4 & 4 \\ -2 & -2 & 0 & 6 \end{bmatrix}$. Left multiplication by A defines a homomorphism φ of abelian groups from $\mathbb{Z}^4$ to $\mathbb{Z}^3$. Use the diagonalization of A to find a basis $\{w_1, w_2, w_3\}$ of $\mathbb{Z}^3$ and integers $\{d_1, \dots d_s\}$ ($s \le 3$), such that $\{d_1 w_1, \dots, d_s w_s\}$ is a basis of range(φ). (Hint: Compute invertible matrices $P \in \mathrm{Mat}_3(\mathbb{Z})$ and $Q \in \mathrm{Mat}_4(\mathbb{Z})$ such that $A' = PAQ$ is diagonal. Rewrite this as $P^{-1}A' = AQ$.)

M.4.8. Adopt the notation of Exercise M.4.5. Observe that the kernel of φ is the set of $\sum_j x_j v_j$ such that

$$A \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = 0.$$

That is the kernel of φ can be computed by finding the kernel of A (in $\mathbb{Z}^n$). Use the diagonalization $A' = PAQ$ to find a description of ker(A). Show, in fact, that the kernel of A is the span of the last $n - s$ columns of Q, where $A' = \mathrm{diag}(d_1, d_2, \dots, d_s, 0, \dots, 0)$.

M.4.9. Set $A = \begin{bmatrix} 2 & 5 & -1 & 2 \\ -2 & -16 & -4 & 4 \end{bmatrix}$. Find a basis $\{v_1, \dots, v_4\}$ of $\mathbb{Z}^4$ and integers $\{a_1, \dots, a_r\}$ such that $\{a_1 v_1, \dots, a_r v_r\}$ is a basis of $\ker(A)$. (Hint: If s is the rank of the range of A, then $r = 4 - s$. Moreover, if $A' = PAQ$ is the Smith normal form of A, then $\ker(A)$ is the span of the last r columns of Q, that is the range of the matrix Q' consisting of the last r columns of Q. Now we have a new problem of the same sort as in Exercise M.4.7.)

M.5. Finitely generated Modules over a PID, part II.

Consider a finitely generated module M over a principal ideal domain R. Let $x_1, \dots, x_n$ be a set of generators of minimal cardinality. Then M is the homomorphic image of a free R–module of rank n. Namely consider a free R module F with basis $\{f_1, \dots, f_n\}$. Define an R–module homomorphism from F onto M by $\varphi(\sum_i r_i f_i) = \sum_i r_i x_i$. Let N denote the kernel of φ. According to Theorem M.4.12, N is free of rank $s \le n$, and there exists a basis $\{v_1, \dots, v_n\}$ of F and nonzero elements $d_1, \dots, d_s$ of R such that $\{d_1 v_1, \dots, d_s v_s\}$ is a basis of N and d_i divides d_j for $i \le j$. Therefore

$$M \cong F/N = (Rv_1 \oplus \cdots \oplus Rv_n)/(Rd_1 v_1 \oplus \cdots \oplus Rd_s v_s)$$

Lemma M.5.1. *Let $A_1, \dots, A_n$ be R–modules and $B_i \subseteq A_i$ submodules. Then*

$$(A_1 \oplus \cdots \oplus A_n)/(B_1 \oplus \cdots \oplus B_n) \cong A_1/B_1 \oplus \cdots \oplus A_n/B_n.$$

Proof. Consider the homomorphism of $A_1 \oplus \cdots \oplus A_n$ onto $A_1/B_1 \oplus \cdots \oplus A_n/B_n$ defined by $(a_1, \dots, a_n) \mapsto (a_1 + B_1, \cdots, a_n + B_n)$. The kernel of this map is $B_1 \oplus \cdots \oplus B_n \subseteq A_1 \oplus \cdots \oplus A_n$, so by the isomorphism theorem for modules,

$$(A_1 \oplus \cdots \oplus A_n)/(B_1 \oplus \cdots \oplus B_n) \cong A_1/B_1 \oplus \cdots \oplus A_n/B_n.$$

■

Observe also that $Rv_i/Rd_i v_i \cong R/(d_i)$, since

$$r \mapsto rv_i + Rd_i v_i$$

is a surjective R–module homomorphism with kernel (d_i). Applying Lemma M.5.1 and this observation to the situation described above gives

$$\begin{aligned} M &\cong Rv_1/Rd_1 v_1 \oplus \cdots \oplus Rv_s/Rd_s v_s \oplus Rv_{s+1} \cdots \oplus Rv_n \\ &\cong R/(d_1) \oplus \cdots \oplus R/(d_s) \oplus R^{n-s}. \end{aligned}$$