

## .1 Homomorphisms of free modules, I

**Problem .1.1.** Prove that the subset of  $\mathcal{M}_2(R)$  consisting of matrices of the form

$$\begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}$$

is a group under matrix multiplication and is isomorphic to  $(R, +)$ .

*Solution.* It is evident that the identity of this group is the identity matrix  $I_2$ . Furthermore, it is closed under multiplication:

$$\begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ r+s & 1 \end{pmatrix}$$

and since  $R$  is closed under addition, this matrix is contained in the group. The multiplication makes it evident that inverse elements have the form

$$\begin{pmatrix} 1 & 0 \\ -r & 1 \end{pmatrix}$$

where  $-r$  is the additive inverse of  $r \in R$ . The isomorphism is also evident; simply identify

$$r \rightarrow \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}$$

and the inverse homomorphism is just as clear.  $\square$

**Problem .1.2.** Prove that matrix multiplication is associative.

*Solution.* Let  $A$  be a  $m \times n$  matrix,  $B$  a  $n \times p$  matrix, and  $C$  a  $p \times q$  matrix. Let  $R = AB$  and  $S = (AB)C$ . We have

$$\begin{aligned} s_{ij} &= \sum_{k=1}^p r_{ik} c_{kj} \\ &= \sum_{k=1}^p \left( \sum_{l=1}^n a_{il} b_{lk} \right) c_{kj} \\ &= \sum_{k=1}^p \sum_{l=1}^n a_{il} b_{lk} c_{kj} \end{aligned}$$

where the third equality follows from distributivity of multiplication over addi-

tion in  $R$ . Now let  $R = BC$  and  $S = A(BC)$ . We have

$$\begin{aligned} s_{ij} &= \sum_{l=1}^n a_{il} r_{lj} \\ &= \sum_{l=1}^n a_{il} \left( \sum_{k=1}^p b_{lk} c_{kj} \right) \\ &= \sum_{l=1}^n \sum_{k=1}^p a_{il} b_{lk} c_{kj} \end{aligned}$$

where the last equality follows from distributivity of multiplication over addition. Finally, the associativity of multiplication and commutativity of addition in  $R$  shows that these two sums are equal, so  $(AB)C = A(BC)$ .  $\square$

**Problem .1.3.** Prove that both  $\mathcal{M}_n(R)$  and  $\text{Hom}_R(R^n, R^n)$  are  $R$ -algebras in a natural way and the bijection  $\text{Hom}_R(R^n, R^n) \cong \mathcal{M}_n(R)$  of Corollary 2.2 is an isomorphism of  $R$ -algebras. In particular, if the matrix  $M$  corresponds to the homomorphism  $\varphi : R^n \rightarrow R^n$ , then  $M$  is invertible in  $\mathcal{M}_n(R)$  if and only if  $\varphi$  is an isomorphism.

*Solution.* Indeed,  $\mathcal{M}_n(R)$  is a ring under component addition and matrix multiplication. It is an  $R$ -algebra because for all  $r \in R$  and  $A, B \in \mathcal{M}_n(R)$ , we have

$$r \cdot (AB) = (r \cdot A)B = A(r \cdot B)$$

by the properties of scalar multiplication of matrices. Showing that  $\text{Hom}_R(R^n, R^n)$  is an  $R$ -algebra amounts to a similar, but more notationally heavy, computation. Recall that the bijection  $\phi$  between the two sets sends a matrix  $A$  to the homomorphism  $\varphi$  defined as  $\varphi(v) = Av$ . To show it is an isomorphism, we only need to show that it is an algebra homomorphism. Indeed, we have (with slight abuse of notation at some points)

- $\phi(I_n)(v) = I_n v = \text{id}$
- $\phi(r \cdot A)(v) = (r \cdot A)(v) = r \cdot (Av) = r \cdot \varphi(A)$
- $\phi(A + B)(v) = (A + B)(v) = Av + Bv = \varphi(A) + \varphi(B)$
- $\phi(AB)(v) = (AB)(v) = A(Bv) = \varphi(A) \circ \varphi(B)$

so the bijection is a homomorphism of  $R$ -algebras, making it an isomorphism. The statement regarding when a matrix is invertible follows immediately. I am curious as to how this aligns with the determinant.  $\square$

**Problem .1.4.** Prove Corollary 2.2.

**Corollary 2.2.** *The correspondence introduced in Lemma 2.1 gives an isomorphism of  $R$ -modules*

$$\mathcal{M}_{m,n}(R) \cong \text{Hom}_R(R^n, R^m).$$

*Solution.* Indeed, the correspondence in Lemma 2.1 is bijective; all matrices  $M \in \mathcal{M}_{m,n}(R)$  are mapped to a homomorphism  $\varphi \in \text{Hom}_R(R^n, R^m)$  and all homomorphisms are mapped to a matrix. We checked above that the two sets are isomorphic as  $R$ -algebras so they must be isomorphic as  $R$ -modules.  $\square$

**Problem .1.5.** Give a formal argument proving Proposition 2.7.

**Proposition 2.7.** *Two matrices  $P, Q \in \mathcal{M}_{m,n}(R)$  are equivalent if  $Q$  may be obtained from  $P$  by a sequence of elementary operations.*

*Solution.* We will only treat the case of elementary row operations. To switch the  $i$ - and  $j$ -th rows of an  $m \times n$  matrix, consider the identity matrix with the  $i$ - and  $j$ -th rows switched. Similarly, to add a multiple of the  $i$ -th row to the  $j$ -th row, consider the identity matrix with the entry  $c$  at position  $i, j$ . To multiply all entries in the  $i$ -th row of a matrix by a unit of  $R$ , consider the identity matrix with the entry in the  $i$ -th row replaced by a unit  $r$ . We verify that each of these matrices is invertible.

In the first case, we show the corresponding homomorphism is an isomorphism. Suppose we have two vectors  $u$  and  $v$  such that  $\varphi(u) = \varphi(v)$ . Then certainly switching the corresponding rows of these vectors preserves equality. Similarly, all vectors in  $R^n$  are in the image of  $\varphi$  by simply switching the rows of the desired elements.

In the second case, we explicitly construct an inverse matrix. Namely, consider the identity matrix with the entry  $-c$  at position  $i, j$ . Clearly this subtracts the multiple of the  $i$ -th row from the  $j$ -th row and hence inverts the transformation of the original matrix.

For the third example, we use the fact that  $r$  is a unit and hence has an inverse  $r^{-1}$ . Then the identity matrix with the entry in the  $i$ -th row replaced by  $r^{-1}$  is an explicit realization of the inverse.

Since each of these matrices is invertible, the corresponding homomorphisms are all isomorphisms and preserve the “action” of matrices  $P$  and  $Q$ .  $\square$

**Problem .1.6.** A matrix with entries in a field is in *row echelon form* if

- its nonzero rows are all above the zero rows and
- the leftmost nonzero entry of each row is 1, and it is strictly to the right of the leftmost nonzero entry of the row above it.

The matrix is further in *reduced* row echelon form if

- the leftmost nonzero entry of each row is the only nonzero entry in its column.

The leftmost nonzero entries in a matrix in row echelon form are called *pivots*.

Prove that any matrix with entries in a field can be brought into reduced echelon form by a sequence of elementary operations on *rows*. (This is what is more properly called *Gaussian elimination*.)

*Solution.* Let  $A = (a_{ij})$  be a  $m \times n$  matrix over a field. We start by appropriately switching all zero rows to the bottom of the matrix. Recalling our elementary row operations, we may multiply the first row by  $a_{11}^{-1}$  and subtract necessary multiples of the first row, yielding

$$\begin{pmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

From here, we may repeat by multiplying the second row by  $a_{22}^{-1}$  and subtracting necessary multiples from all rows below it, switching zero rows to the bottom as they appear. This process eventually terminates and yields a matrix in row echelon form.  $\square$

**Problem .1.7.** Let  $M$  be a matrix with entries in a field and in reduced row echelon form (Exercise 2.6). Prove that if a row vector  $\mathbf{r}$  is a linear combination  $\sum a_i \mathbf{r}_i$  of the nonzero rows of  $M$ , then  $a_i$  equals the component of  $\mathbf{r}$  at the position corresponding to the pivot on the  $i$ -th row of  $M$ . Deduce that the nonzero rows of  $M$  are linearly independent.

*Solution.* Let  $b_i$  be the component of  $\mathbf{r}$  at the position corresponding to the pivot of the  $i$ -th row of  $M$ . Suppose the pivot of the  $i$ -th row is located in the  $j$ -th column. Then  $b_i = a_i \cdot 1$  because the only nonzero entry in the  $j$ -th column is 1 (since  $M$  is in reduced echelon form). Thus,  $a_i = b_i$ .

If  $\mathbf{r}$  is the zero vector, then it must be the case that each  $a_i$  is 0. That is, the nonzero rows of  $M$  are linearly independent. Thus,  $\square$

**Problem .1.8.** Two matrices  $M, N$  are *row-equivalent* if  $M = PN$  for an invertible matrix  $P$ . Prove that this is indeed an equivalence relation, and that two matrices with entries in a field are row-equivalent if and only if one may be obtained from the other by a sequence of elementary operations on rows.

*Solution.* Let  $M \sim N$  denote row-equivalent matrices. Clearly  $M \sim N$  as  $M = IM$ . If  $M \sim N$  then we have  $M = PN$  for some invertible matrix  $P$ . But then we have  $N = P^{-1}M$  so  $N \sim P$ . Finally, if  $M \sim N$  and  $N \sim P$ , we have

$M = RN$  and  $P = SN$ . Then  $M = RS^{-1}P$ , and  $RS^{-1}$  is clearly invertible so  $M \sim P$ . Thus, row-equivalence is an equivalence relation.

The second part of the claim follows from the fact that  $GL_n(k)$ , the group of invertible matrices of a field, is generated by elementary matrices, which are themselves invertible (obviously).  $\square$

**Problem .1.9.** Let  $k$  be a field, and consider row-equivalence (Exercise 2.8) on the set of  $m \times n$  matrices  $\mathcal{M}_{m,n}(k)$ . Prove that each equivalence class contains exactly one matrix in reduced row echelon form (Exercise 2.6). (Hint: To prove uniqueness, argue by contradiction. Let  $M, N$  be different row-equivalent reduced row echelon matrices; assume that they have the minimum number of columns with this property. If the leftmost column at which  $M$  and  $N$  differ is the  $k$ -th column, use the minimality to prove that  $M, N$  may be assumed to be of the form

$$\left( \begin{array}{c|c} I_{k-1} & * \\ \hline 0 & * \end{array} \right) \quad \text{or} \quad (I_{k-1} \mid *).$$

Use Exercise 2.7 to obtain a contradiction.)

The unique matrix in reduced row echelon form that is row-equivalent to a given matrix  $M$  is called the *reduced echelon form* of  $M$ .

*Solution.* Certainly each equivalence class is nonempty as it contains a matrix of the form

$$\left( \begin{array}{c|c} I_{k-1} & * \\ \hline 0 & 0 \end{array} \right)$$

Now suppose  $M, N$  are different row equivalent matrices in reduced row echelon form with the minimum number of columns. Suppose the leftmost column at which  $M$  and  $N$  differ is the  $k$ -th column. Construct two matrices  $M'$  and  $N'$  by selecting all columns with pivot elements to the left of the  $k$ -th column, along with the  $k$ -th column. Then we have  $M'$  and  $N'$  are of the form

$$\left( \begin{array}{c|c} I_{k-1} & * \\ \hline 0 & * \end{array} \right) \quad \text{or} \quad (I_{k-1} \mid *)$$

(the case depends on whether  $k > n$ ). Then  $M'$  and  $N'$  are row equivalent since we are only adjusting columns and we assumed  $M$  and  $N$  are row equivalent. In either case, the rows of  $M'$  and  $N'$  are linearly independent so it must be the case that  $M' = N'$  and  $M = N$ .  $\square$

**Problem .1.10.** The *row space* of a matrix  $M$  is the span of its rows; the *column space* of  $M$  is the span of its columns. Prove that row-equivalent matrices have the same row space and isomorphic column spaces.

*Solution.* Recall that  $M$  and  $N$  are row-equivalent if there exists an invertible matrix  $P$  such that  $M = PN$ . Then the rows of  $M$  are a linear combination of

the rows of  $N$ . If  $x$  is in the span of the rows of  $M$  then it is a linear combination of the rows of  $M$ . But then it is also a linear combination of the rows of  $N$  so the row space of  $M$  is a subset of the row space of  $N$ . Similarly, since  $N = P^{-1}M$ , the row space of  $N$  is a subset of the row space of  $M$  so the two are equal.

By Exercise 2.9,  $M$  and  $N$  have the same reduced echelon form. Furthermore, the dimension of the column space of a matrix is given by the number of pivot columns in its reduced echelon form since row operations preserve linear relations between columns. Thus, the column space of  $M$  and  $N$  have the same dimension so they are isomorphic as vector spaces.  $\square$

**Problem .1.11.** Let  $k$  be a field and  $M \in \mathcal{M}_{m,n}(k)$ . Prove that the dimension of the space spanned by the rows of  $M$  equals the number of nonzero rows in the reduced echelon form of  $M$  (cf. Exercise 2.9).

*Solution.* Note that the reduced echelon form of  $M$  can be obtained through a sequence of elementary operations. That is, if  $N$  is the reduced echelon form of  $M$ , then we have  $N = PM$  so the two are row-equivalent. By Exercise 2.10, the two matrices have the same row space. Finally, the dimension of the row space is equal to the number of nonzero rows in the reduced echelon form of  $M$  (since the nonzero rows contain pivot elements). Thus, the dimension of the row space of  $M$  is equal to the number of nonzero rows in  $N$ .  $\square$

**Problem .1.12.** Let  $k$  be a field, and consider row-equivalence on  $\mathcal{M}_{m,n}(k)$  (Exercise 2.8). By Exercise 2.10, row-equivalent matrices have the same row space. Prove that, conversely, there is exactly one row-equivalence class in  $\mathcal{M}_{m,n}(k)$  for each subspace of  $k^n$  of dimension  $\leq m$ .

*Solution.* Given a subspace  $V$  of dimension  $d \leq n$ , we know the row-equivalence class is nonempty since it contains the matrix whose rows are a basis of  $V$ , call it  $A$ . Suppose we have a second matrix  $B$  whose row space is  $V$ . Since the two are row-equivalent, we have that for all  $x \in k^n$ , there exists  $y \in k^n$  such that  $x^t A = y^t B$ . In particular, let  $e_i \in k^n$  for  $1 \leq i \leq n$  denote the standard basis of  $k^n$  and let  $y_i \in k^n$  satisfy  $e_i^t A = y_i^t B$  (in such a way that the  $y_i$  are linearly independent). Construct a matrix  $P$  such that the  $i$ -th row of  $P$  is  $y_i$ . Then clearly we have  $A = PB$  for an invertible matrix  $P$  so the two are row-equivalent.  $\square$

**Problem .1.13.** The set of subspaces of given dimension in a fixed vector space is called a *Grassmannian*. In Exercise 2.12 you have constructed a bijection between the Grassmannian of  $r$ -dimensional subspaces of  $k^n$  and the set of reduced row echelon matrices with  $n$  columns and  $r$  nonzero rows.

For  $r = 1$ , the Grassmannian is called the *projective space*. For a vector space  $V$ , the corresponding projective space  $\mathbb{P}V$  is the set of ‘lines’ (1-dimensional

subspaces) in  $V$ . For  $V = k^n$ ,  $\mathbb{P}V$  may be denoted  $\mathbb{P}_k^{n-1}$ , and the field  $k$  may be omitted if it is clear from the context. Show that  $\mathbb{P}_k^{n-1}$  may be written as a union  $k^{n-1} \cup k^{n-2} \cup \dots \cup k^1 \cup k^0$ , and describe each of these subsets ‘geometrically’.

Thus,  $\mathbb{P}^{n-1}$  is the union of  $n$  ‘cells’, the largest one having dimension  $n-1$  (accounting for the choice of notation). Similarly, all Grassmannians may be written as unions of cells. These are called *Schubert cells*.

Prove that the Grassmannian of  $(n-1)$ -dimensional subspaces of  $k^n$  admits a cell decomposition entirely analogous to that of  $\mathbb{P}_k^{n-1}$ . (This phenomenon will be explained in Exercise VIII.5.17.)

*Solution.* Think of  $k^{n+1}$  as  $k^n \times k$ . Then each line through the origin either intersects  $k^n \times \{1\}$  at a unique point or it lies in the hyperplane  $k^n \times \{0\}$ . Thus, the lines in  $k^{n+1}$  are a union of  $k^n \times \mathbb{P}^{n-1}$ . Repeating inductively shows that  $\mathbb{P}_k^{n-1}$  is a union  $k^{n-1} \cup \dots \cup k^1 \cup k^0$  (where the last set is included for the origin itself). Each of these subsets is the hyperplane of lines in  $k^m$ . The most tangible example is  $\mathbb{R}^3$  and  $\mathbb{RP}^2$ .

When working with the Grassmannian of  $n$ -dimensional subspaces of  $k^{n+1}$ , simply consider the line normal to the  $n$ -dimensional hyperplane. Clearly the two are in bijection so the cell decomposition is simply reversed. For a more explicit example, consider  $\mathbb{R}^3$  and the Grassmannian of 2-dimensional subspaces, or planes. Each plane through the origin has a normal line, and this set of normal lines is equivalent to  $\mathbb{RP}^2$ . The lines which intersect  $\mathbb{R}^2 \times \{0\}$  correspond to planes which contain the vertical copy of  $\mathbb{R}$ . The intersection of planes not in this set is  $\mathbb{R}^0$ , while the intersection of the planes in this set is  $\mathbb{R}^1$ . Repeating once more with the set of planes whose normal lines intersect  $\mathbb{R} \times \{0\}$  yields  $\mathbb{R}^2$  since there is only one such plane.  $\square$

**Problem .1.14.** Show that the Grassmannian  $\text{Gr}_k(2, 4)$  of 2-dimensional subspaces of  $k^4$  is the union of 6 Schubert cells:  $k^4 \cup k^3 \cup k^2 \cup k^2 \cup k^1 \cup k^0$ . (Use Exercise 2.12; list all the possible reduced echelon forms.)

*Solution.* A 2-dimensional subspace of  $k^4$  corresponds to a reduced echelon matrix of rank 2. There are exactly 6 of these, namely:

$$\begin{pmatrix} 1 & 0 & * & * \\ 0 & 1 & * & * \end{pmatrix}, \quad \begin{pmatrix} 1 & * & 0 & * \\ 0 & 0 & 1 & * \end{pmatrix}, \quad \begin{pmatrix} 1 & * & * & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 & 0 & * \\ 0 & 0 & 1 & * \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & * & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Thus,  $\text{Gr}_k(2, 4)$  decomposes into exactly 6 Schubert cells. Note that the matrix with  $m$  free elements corresponds to the Schubert cell  $k^m$ . This is because each subspace is characterized by the values of the free elements. In particular, the sixth matrix corresponds with  $k^0$  while the third matrix corresponds with  $k^2$ .  $\square$

**Problem .1.15.** Prove that a square matrix with entries in a field is invertible if and only if it is equivalent to the identity, if and only if it is row-equivalent to the identity, if and only if its reduced echelon form is the identity.

*Solution.* Let  $M$  be a square matrix with entries in a field. If  $M$  is invertible, then it has an inverse  $M^{-1}$  such that  $I = M^{-1}M$ . Since  $M^{-1}$  is invertible,  $M$  is row-equivalent to the identity.

If  $M$  is row-equivalent to the identity, then there exists an invertible matrix  $P$  such that  $I = PM$ . Since  $P$  is invertible, it is a product of elementary matrices. That is, a sequence of row operations on  $P$  yields the identity, which is in reduced echelon form.

Finally, suppose the reduced echelon form of  $M$  is the identity. Then there is a sequence of row operations which transform  $M$  into the identity. This sequence of row operations can be expressed as a product of elementary matrices. This product of elementary matrices is the inverse of  $M$ , so  $M$  is invertible.  $\square$

**Problem .1.16.** Prove Proposition 2.10.

**Proposition 2.10.** *Over a field, every  $m \times n$  matrix is equivalent to a matrix of the form*

$$\left( \begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array} \right)$$

(where  $r \leq \min(m, n)$  and ‘0’ stands for null matrices of appropriate sizes).

*Solution.* Let  $M$  be an  $m \times n$  matrix over a field with rank  $r$ . After appropriate row operations, we may assume the first  $r$  rows of  $M$  are linearly independent. Then we may apply Gaussian elimination to the first  $r$  rows to obtain a matrix of the form

$$\left( \begin{array}{c|c} I_r & * \\ \hline * & * \end{array} \right)$$

Add appropriate linear combinations of the first  $r$  columns to eliminate the top right block. Since the remaining  $m - r$  rows are linearly dependent, they must be a linear combination of the first  $r$  rows. Thus, the bottom right block must also be zero. Finally, the proper linear combination of the first  $r$  rows will eliminate the bottom left block. What remains is a matrix of the form stated in the problem.  $\square$

**Problem .1.17.** Prove Proposition 2.11.

**Proposition 2.11.** *Let  $R$  be a Euclidean domain, and let  $P \in \mathcal{M}_{m,n}(R)$ . Then  $P$  is equivalent to a matrix of the form*

$$\left( \begin{array}{ccc|c} d_1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & d_r & 0 \\ \hline 0 & \cdots & 0 & 0 \end{array} \right)$$



with  $d_1 \mid \cdots \mid d_r$ .

*Solution.* Let  $M$  be an  $m \times n$  matrix over a Euclidean domain with rank  $r$ . After appropriate row operations, we may assume the first  $r$  rows of  $M$  are linearly independent. Following the Euclidean algorithm, we may add multiples of other rows to ensure that  $a_{11}$  is the gcd of the entries in the first column. Adding appropriate multiples of this row to the remaining rows and multiples of this column to the remaining columns yields a matrix of the form

$$\left( \begin{array}{c|ccc} d_1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & M' & \\ 0 & & & \end{array} \right)$$

where  $M'$  is an  $(m-1) \times (n-1)$  matrix with rank  $r-1$ .

Repeating this process on  $M'$  and on subsequent matrices yields a matrix of the form stated in the problem. Now we only need to show that  $d_1 \mid \cdots \mid d_r$ , for which we take inspiration from the text. Indeed, suppose  $d_i \nmid d_{i+1}$ . Then we may add the  $(i+1)$ -th row to the  $i$ -th row and repeat the process. Ultimately, we must reach the condition  $d_i \mid d_{i+1}$ .  $\square$

**Problem .1.18.** Suppose  $\alpha : \mathbb{Z}^3 \rightarrow \mathbb{Z}^2$  is represented by the matrix

$$\begin{pmatrix} -6 & 12 & 18 \\ -15 & 36 & 54 \end{pmatrix}$$

with respect to the standard bases. Find bases of  $\mathbb{Z}^3, \mathbb{Z}^2$  with respect to which  $\alpha$  is given by a matrix of the form obtained in Proposition 2.11.

*Solution.* Applying the algorithm described above, we find that applying the following change of basis yields a matrix in the Smith normal form:

$$\begin{pmatrix} 2 & -1 \\ 10 & -4 \end{pmatrix} \begin{pmatrix} -6 & 12 & 18 \\ -15 & 36 & 54 \end{pmatrix} \begin{pmatrix} 1 & -2 & 0 \\ 0 & 1 & 3 \\ 0 & -1 & -2 \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 12 & 0 \end{pmatrix}$$

so the above matrices are the bases with which  $\alpha$  is given in the Smith normal form. Interestingly, the inverses of these matrices are not elements of  $\mathbb{Z}^3$  or  $\mathbb{Z}^2$  respectively.  $\square$

**Problem .1.19.** Prove Corollary IV.6.5 again as a corollary of Proposition 2.11. In fact, prove the general fact that every *finitely generated* abelian group is a direct sum of cyclic groups.

*Solution.* Let  $G$  be a finitely generated abelian group. Then  $G$  is a quotient of  $\mathbb{Z}^n$  by a finitely generated free abelian group, say  $F$ , and  $F$  is a free  $\mathbb{Z}$ -module. Consider a matrix  $M$  whose rows are composed of a basis for  $F$ . By Proposition 2.11,  $M$  is equivalent to a matrix in the Smith normal form. That is, there is a basis  $\{d_1e_1, \dots, d_re_r\}$  for  $F$  such that  $d_i \mid d_{i+1}$ . Then

$$F = d_1\mathbb{Z} \oplus d_2\mathbb{Z} \oplus \cdots \oplus d_r\mathbb{Z}$$

so we find

$$G = \frac{\mathbb{Z}^n}{F} = \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_r\mathbb{Z}}$$

and  $G$  is a direct sum of cyclic groups. □