

# The Structure Theorem for Finitely Generated Abelian Groups

Mark Cerenzia

29 July 2009

## Abstract

This paper provides a thorough explication of the Structure Theorem for Abelian groups and of the background information necessary to prove it.

The outline of this paper is as follows. We first consider some theorems related to abelian groups and to  $R$ -modules. In this section we see that every finitely generated abelian group is the epimorphic image of a finitely generated free abelian group. Here also submodules of a finitely generated module over a *principal ideal domain* are shown to be finitely generated as well. Notably, this proposition is proved by examining a short exact sequence of  $R$ -modules. Then, in the next section, we learn a procedure for diagonalizing  $m \times n$  matrices with products of elementary matrices. Moreover, these products can be interpreted as change-of-basis matrices. We will see the relevance of this procedure in the proof of the Stacked Basis Theorem. This theorem shows that for a subgroup of a finitely generated group, there is a basis of that subgroup whose elements are multiples of the basis elements of the group. Finally, the propositions enumerated in these sections allow us to prove and understand the Structure Theorem for Abelian Groups. This theorem asserts that every finitely generated abelian group is the direct sum of cyclic groups and of a free abelian group. Throughout this paper, examples and definitions will be included to aid the reader in understanding the relevant concepts.

## 1 Abelian Groups and Modules Over Principle Ideal Domains

As mentioned in the introduction, this section will present proofs for some important results relating to Abelian Groups and R-modules. These results set the foundation for our progression to the Structure Theorem.

**Proposition 1.1.** *Let  $G$  be an abelian group generated by  $\{g_i\}_{i=1}^m$ . Let  $F$  be a free abelian group with basis  $\{f_i\}_{i=1}^m$ . Then there exists an epimorphism  $\varphi : F \rightarrow G$  such that*

$$\varphi : (f_i) = g_i, \forall i.$$

*Proof.* First, let  $x \in F$  Then  $x = \sum_{i=1}^m c_i f_i$ . Define  $\varphi(x)$  as

$$\varphi(x) = \varphi\left(\sum_{i=1}^m c_i f_i\right) = \sum_{i=1}^m \varphi(c_i f_i) = \sum_{i=1}^m c_i g_i.$$

Thus,  $\varphi$  is well defined. Now we show that  $\varphi$  is a homomorphism. For  $x = \sum_{i=1}^m c_i f_i$  and  $y = \sum_{i=1}^m d_i f_i$ , we get

$$\begin{aligned} \varphi(x) + \varphi(y) &= \varphi\left(\sum_{i=1}^m c_i f_i\right) + \varphi\left(\sum_{i=1}^m d_i f_i\right) = \sum_{i=1}^m c_i g_i + \sum_{i=1}^m d_i g_i = \sum_{i=1}^m (d_i + c_i) g_i = \\ &= \varphi\left(\sum_{i=1}^m (d_i + c_i) f_i\right) = \varphi\left(\sum_{i=1}^m c_i f_i + \sum_{i=1}^m d_i f_i\right) = \varphi(x + y). \end{aligned}$$

Next we show that  $\varphi$  is surjective. Let  $a \in G$ . Then  $a = \sum_{i=1}^m e_i g_i$  for some integers  $e_i$ . Now let  $b \in F$  such that  $b = \sum_{i=1}^m e_i f_i$ . Then

$$\varphi(b) = \varphi\left(\sum_{i=1}^m e_i f_i\right) = \sum_{i=1}^m e_i g_i = a.$$

□

We are now going to show that a subgroup of a finitely generated abelian group is also finitely generated. But we need some preliminary information. First we define free abelian groups and show that abelian groups and  $\mathbb{Z}$ -modules are equivalent concepts. Next we provide a definition of *principal ideal domains* and show that  $\mathbb{Z}$  is one. Then we present a lemma that plays a significant role in proving the main proposition. The proof of this lemma will perhaps be noticeably different than those found in other texts.

**Definition 1.2.** an abelian group is *free* if it has a basis.

**Proposition 1.3.** *Abelian groups and  $\mathbb{Z}$ -modules are equivalent concepts.*

*Proof.* For, any abelian group can be made into a module over  $\mathbb{Z}$  by the rules  $nv = v + \cdots + v =$  "n times v" and  $(-n)v = -(nv)$ .  $\square$

**Definition 1.4.** an integral domain  $R$  is a *principal ideal domain* (PID) if every ideal of  $R$  is principal.

**Proposition 1.5.** *The ring of integers  $\mathbb{Z}$  is a principal ideal domain.*

*Proof.* Since every subgroup of  $\mathbb{Z}$  is of the form  $n\mathbb{Z} = (n)$ , these subgroups are additive cyclic groups generated by a single element. These subgroups are exactly principal ideals. Hence, every ideal of  $\mathbb{Z}$  is principal.  $\square$

**Lemma 1.6.** *Let  $R$  be a PID. Let  $0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0$  be a short exact sequence of modules over  $R$ . Suppose  $M'$  and  $M''$  are free modules of rank  $j$  and  $k$ , respectively. Then  $M$  is free of rank  $j + k$ .*

*Proof.* We show that a set  $\{x_i\}_{i=1}^{j+k}$  is a basis for  $M$ . To achieve this, we prove first that this set generates  $M$  and then that the elements  $x_i$  are independent.

Let  $\{z_i\}_{i=1}^j$  be a basis for  $M'$  and  $\{y_i\}_{i=j+1}^{j+k}$  a basis for  $M''$ . Then choose  $\{x_i\}_{i=1}^{j+k}$  in  $M$  such that  $f(z_i) = x_i$  for  $1 \leq i \leq j$  and  $g(x_i) = y_i$  for  $j+1 \leq i \leq j+k$ . Let  $a \in M$ . Then  $g(a) = \sum_{i=j+1}^{j+k} r_i y_i$  for some integers  $r_i$ . Now let  $b \in M$  be defined as  $b = a - \sum_{i=j+1}^{j+k} r_i x_i$ . Then  $b$  is in  $\ker g$ . Since this is an exact sequence, there is an element in  $M'$ , say  $c = \sum_{i=1}^j r_i z_i$ , such that  $f(c) = b$ . Then  $f(c) = \sum_{i=1}^j r_i x_i$ . But this implies that

$$a = \sum_{i=1}^j r_i x_i + \sum_{i=j+1}^{j+k} r_i x_i = \sum_{i=1}^{j+k} r_i x_i.$$

Thus, the set  $\{x_i\}_{i=1}^{j+k}$  generates  $M$ .

Now we check that the elements  $x_i$  are independent. Consider  $\sum_{i=1}^{j+k} r_i x_i = 0$ , where  $r_i \in R, \forall i$ . Then we have  $\sum_{i=1}^{j+k} r_i g(x_i) = \sum_{i=j+1}^{j+k} r_i y_i = 0$  in  $M''$ . Since  $\{y_i\}_{i=j+1}^{j+k}$  is a basis,  $r_i = 0$  for  $j+1 \leq i \leq j+k$ . Likewise,  $f(\sum_{i=1}^j r_i z_i) = \sum_{i=1}^j r_i x_i = 0$ , which implies that  $r_i = 0$  for  $1 \leq i \leq j$ . Since the elements  $x_i$  are independent, it thus follows that the set  $\{x_i\}_{i=1}^{j+k}$  forms a basis for  $M$ .  $\square$

**Proposition 1.7.** *Let  $R$  be a principal ideal domain, let  $F$  be a finitely generated free  $R$ -module, and let  $N$  be a submodule of  $F$ . Then  $N$  is also a free  $R$ -module of rank at most  $m$ .*

*Proof.* The proof is by induction on  $m$ . We may as well assume that  $F = R^m$  since these two are isomorphic. First note that a submodule of  $R^1$  is simply an ideal of  $R$ . But since  $R$  is a principal ideal domain, each ideal is generated by one element and thus the proposition holds for  $R^1$ . Now suppose  $m > 1$  and consider the projection

$$\pi : R^m \rightarrow R^{m-1}$$

given by eliminating the last entry:

$$\pi(a_1, \dots, a_m) = (a_1, \dots, a_{m-1}).$$

Its kernel is isomorphic to  $R^1$ . Now let  $N$  be a submodule of  $R^m$ . By induction,  $\pi(N)$  is free of rank  $\leq m - 1$ . Also,  $\ker \pi|_N = (N \cap \ker \pi)$  is a submodule of  $\ker \pi$ , so it is free of rank  $\leq 1$ . If we let  $M' = (N \cap \ker \pi)$  and let  $M'' = \pi(N)$  in lemma 1.4, we can conclude that  $N$  is free of rank at most  $m$ , as required.  $\square$

## 2 Diagonalization of Integer Matrices

We turn now to a discussion of the diagonalization procedure for an  $m \times n$  matrix  $A$  with integer entries. We first define elementary and diagonal matrices. We then show how they may be used to form products that can diagonalize a matrix  $A$ .

**Definition 2.1.** an  $n \times n$  integer matrix is *elementary* if it is the result of one and only one of the following row or column operations on the identity matrix:

- 1) Add an integer multiple of one row to another or an integer multiple of one column to another
- 2) Multiply a row or column by a unit other than 1.

**Note 2.1.** Operation (1) can effect a third operation, that of interchanging two rows or two columns.

**Note 2.2.** The only unit other than 1 in  $\mathbb{Z}$  is -1.

**Definition 2.2.** a matrix A is called *diagonal* if every entry  $a_{ij}$  where  $i \neq j$  is zero.

**Example 2.3.** The following matrices are diagonal:

$$\begin{pmatrix} 2 & 0 \\ 0 & 7 \end{pmatrix}, \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 9 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 8 & 0 \\ 0 & 5 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix}.$$

If  $A'$  is obtained from A by elementary *row* operations, then  $A' = QA$  for some  $Q \in GL_m(\mathbb{Z})$ . Likewise, if  $A'$  is obtained from A by elementary *column* operations, then  $A' = AP$  for some  $P \in GL_n(\mathbb{Z})$ . Matrices Q and P are themselves products of elementary matrices.

We will now show that A can be *diagonalized*, i.e., made diagonal by row and column operations, such that the diagonal entries  $d_i$  satisfy  $d_i \mid d_{i+1}$  for  $1 \leq i < \min(m, n)$ .

**Proposition 2.4.** *Let A be an  $m \times n$  matrix with integer entries. Then there exist matrices  $Q \in GL_m(\mathbb{Z})$  and  $P \in GL_n(\mathbb{Z})$  so that  $A' = QAP^{-1}$  is diagonal. Moreover, the diagonal entries  $d_i$  in  $a_{ii}$  of A can be chosen to be nonnegative and can satisfy  $d_i \mid d_{i+1}$ , for  $1 \leq i < \min(m, n)$ .*

*Proof.* The process is based on repeated division with remainder. The reader can easily see that right and left multiplication by products of elementary matrices  $Q \in GL_m(\mathbb{Z})$  and  $P \in GL_n(\mathbb{Z})$  can effect row and column operations on A. So we enumerate three steps to follow for diagonalizing A:

Step 1: Move the nonzero entry of A with smallest absolute value to position  $a_{11}$  and, if necessary, make it positive.

Step 2: Choose a nonzero entry  $a_{i1}$  in the first column, with  $i > 1$  fixed, and divide by  $a_{11}$ :

$$a_{i1} = a_{11}q + r, \text{ where } 0 \leq r < a_{11}.$$

Then subtract  $q$  times the first row from the  $i$ th row. There are two possibilities:

If  $r \neq 0$ , return to step 1.

If  $r = 0$ , then the entry  $a_{i1}$  is a zero, as desired.

Do the same for nonzero entries  $a_{1j}$  with  $j > 1$  in the first row until all the entries contain zeros.

Step 3: Suppose some other diagonal entry  $d_i$  for  $i > 1$  is not divisible by  $a_{11}$ . Then add the  $i$ th column of  $A$  to column 1, producing the entry  $d_i$  in  $a_{i1}$  of the first column. Return to step 2 until the matrix  $A$  is in the required diagonal form.

To show that this third step can be achieved with a finite number of steps, consider a  $2 \times 2$  matrix with diagonal entries  $a, b \in \mathbb{Z}$ . These entries can be changed such that  $d = \gcd(a, b) = ar + bs$  is in  $a_{11}$  and such that  $e = \text{lcm}(a, b) = ax = by$  in  $a_{22}$  for  $r, s, x, y \in \mathbb{Z}$ . We see that this can be done with the following steps:

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \stackrel{Col}{\sim} \begin{pmatrix} a & 0 \\ sb & b \end{pmatrix} \stackrel{Row}{\sim} \begin{pmatrix} a & 0 \\ d & b \end{pmatrix} \stackrel{Row}{\sim} \begin{pmatrix} d & b \\ a & 0 \end{pmatrix} \stackrel{Row}{\sim} \begin{pmatrix} d & b \\ 0 & by \end{pmatrix} \stackrel{Col}{\sim} \begin{pmatrix} d & 0 \\ 0 & by \end{pmatrix} \sim \begin{pmatrix} d & 0 \\ 0 & e \end{pmatrix}.$$

Note that these operations could have been modified so that  $ax$  for some integer  $x$  was in  $a_{22}$ . It is now easy to see that induction can show this procedure to work for any  $n \times n$  matrix. For, with any diagonal matrix

$$A = \begin{bmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_n \end{bmatrix},$$

we may simply focus on the smaller  $2 \times 2$  matrices of  $A$

$$\begin{pmatrix} d_i & 0 \\ 0 & d_{i+1} \end{pmatrix}, \quad 1 \leq i < n$$

on which the same operations exhibited in the base step may be performed. Lastly, we may note that this procedure can be extended to any  $m \times n$  matrix by focusing on the smaller  $k \times k$  matrix, where  $k = \min(m, n)$ . This of course implies that there will be rows or columns of zeros if  $m \neq n$ .  $\square$

**Example 2.5.** To diagonalize the matrix  $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$ , we may perform the following operations in accordance with proposition 2.4:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \stackrel{Col}{\sim} \begin{pmatrix} 1 & 0 & 3 \\ 4 & -3 & 6 \end{pmatrix} \stackrel{Row}{\sim} \begin{pmatrix} 1 & 0 & 3 \\ 0 & -3 & -6 \end{pmatrix} \stackrel{Col}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & -6 \end{pmatrix} \stackrel{Col}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \end{pmatrix}.$$

**Note 2.3.** A significant fact used in this proof was the division algorithm in step 2. This same proof in fact shows that any matrix over a *Euclidean domain* can be diagonalized in this same manner. For principal ideal domains, however, the division algorithm does not necessarily hold. To make this procedure work for matrices with entries from a PID, the second step must be altered.

The diagonalization procedure for integer matrices can be extended to the matrix of a homomorphism of free abelian groups. Once bases are chosen, a homomorphism  $\varphi : J \rightarrow F$  of free abelian groups is described by a matrix, which can be diagonalized by matrices  $Q \in GL_m(\mathbb{Z})$  and  $P \in GL_n(\mathbb{Z})$ . The change of  $A$  to  $A' = QAP^{-1}$  corresponds to a change of bases in  $J$  and  $F$ , as the following theorem asserts:

**Proposition 2.6.** *Let  $\varphi : J \rightarrow F$  be a homomorphism of free abelian groups. Then there exist bases of  $J$  and  $F$  such that the matrix of the homomorphism has the diagonal form with diagonal entries satisfying  $d_i \mid d_{i+1}$ .*

*Proof.* Choose any bases  $B_J = \{j_i\}_{i=1}^n$  for  $J$  and  $B_F = \{f_i\}_{i=1}^m$  for  $F$ . Let  $A = M_{B_F, B_J}(\varphi)$  be the matrix of  $\varphi$  relative to  $B_F$  in the range and to  $B_J$  in the domain. Also let  $A' = QAP^{-1}$ . We know there are matrices  $Q \in GL_m(\mathbb{Z})$  and  $P \in GL_n(\mathbb{Z})$  such that  $QAP^{-1}$  is diagonal. Now let  $B'_J$  be that basis of  $J$  such that

$$P = M_{B'_J, B_J}(id_J).$$

Likewise, let  $B'_F$  be that basis of  $F$  such that

$$Q = M_{B'_F, B_F}(id_F).$$

Since  $\varphi = id_F \circ \varphi \circ id_J$ , we see that

$$M_{B'_F, B'_J}(\varphi) = M_{B'_F, B_F}(id_F) \circ M_{B_F, B_J}(\varphi) \circ M_{B_J, B'_J}(id_J) = QAP = A'.$$

This completes the proof. □

**Theorem 2.7.** *(The Stacked Basis Theorem) Let  $N$  be a subgroup of a finitely generated free abelian group  $F$  of rank  $m$ . Then there exists a basis  $\{f'_i\}_{i=1}^m$  for  $F$  as well as positive integers  $\{d_i\}_{i=1}^n$ , with  $n \leq m$ , such that*

- a)  $\{d_i f'_i\}_{i=1}^n$  is a basis for  $N$ .
- b)  $d_i \mid d_{i+1}$  for  $1 \leq i < n$ .

*Proof.* Let  $N$  be a subgroup of a finitely generated free abelian group  $F$  of rank  $m$ . By proposition 1.7, we know  $N$  is also a free  $R$ -module with rank  $n \leq m$ . Then let  $\{u_i\}_{i=1}^n$  be a basis for  $N$  and  $\{f_i\}_{i=1}^m$  a basis for  $F$ . Also let  $A$  be the matrix which satisfies

$$[u_1, u_2, \dots, u_n] = [f_1, f_2, \dots, f_m]A.$$

By propositions 2.4 and 2.6, we can choose new bases  $\{f'_i\}_{i=1}^m$  for  $F$  and  $\{u'_i\}_{i=1}^n$  for  $N$  defined as

$$[f'_1, f'_2, \dots, f'_m]Q = [f_1, f_2, \dots, f_m]$$

and

$$[u'_1, u'_2, \dots, u'_n]P = [u_1, u_2, \dots, u_n],$$

where  $A' = QAP^{-1}$  is diagonal. Then we have

$$[u'_1, u'_2, \dots, u'_n] = [u_1, u_2, \dots, u_n]P^{-1} \quad (2.1)$$

$$= [f_1, f_2, \dots, f_m]AP^{-1} \quad (2.2)$$

$$= [f'_1, f'_2, \dots, f'_m]QAP^{-1} \quad (2.3)$$

$$= [f'_1, f'_2, \dots, f'_m]A' \quad (2.4)$$

Then  $u'_i = d_i f'_i$ , with diagonal entry  $d_i$  satisfying  $d_i \mid d_{i+1}$  for  $1 \leq i < n$ . Thus  $\{u'_i\}_{i=1}^n = \{d_i f'_i\}_{i=1}^n$  is a basis for  $N$ , as required.  $\square$

### 3 The Structure Theorem for Abelian Groups

The propositions necessary for understanding and proving the Structure Theorem have now been presented. We may turn to the statement and proof of this theorem after some preliminary definitions concerning direct sums of modules. We will see that independence and generation with direct sums of modules are analogous to these concepts with vector spaces.

**Definition 3.1.** Let  $\{W_i\}_{i=1}^k$  be a set of submodules of a module  $V$ .  $V$  is the *direct sum* of submodules  $W_i$  if:

- 1) they *generate*  $V$ :  $V = W_1 + W_2 + \dots + W_k$ ;
- 2) they are *independent*: If  $w_1 + w_2 + \dots + w_k = 0$ , with  $w_i \in W_i$ , then  $w_i = 0$  for each  $i$ .

The symbol  $\oplus$  denotes such sums. Thus if  $V$  is a direct sum of submodules  $W_i$ , then

$$V = W_1 \oplus W_2 \oplus \dots \oplus W_k.$$

**Theorem 3.2.** *The Structure Theorem for Abelian Groups: Let  $G$  be a finitely generated abelian group. Then there exist natural numbers  $\{d_i\}_{i=1}^n$  such that*

- a)  $d_i \mid d_{i+1}$  for  $1 \leq i < n$   
 b)  $G = \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z} \oplus L$ , where  $L$  is a finitely generated free abelian group.

*Proof.* Let  $G$  be a finitely generated abelian group of rank  $m$ . First, by proposition 1.1, there exists a free abelian group  $F$  of rank  $m$  and an epimorphism  $\varphi : F \rightarrow G$ . By the First Isomorphism Theorem, if  $\ker \varphi = N$ , then  $F/N \cong G$ . Moreover, since  $N$  is a subgroup of  $F$ ,  $N$  is free abelian of rank  $n \leq m$ , as proposition 1.7 asserts. Now let  $\{f_i\}_{i=1}^m$  be a basis for  $F$  and  $\{u_i\}_{i=1}^n$  a basis for  $N$ . Since  $F$  and  $N$  are free abelian groups, we know that

$$F = f_1\mathbb{Z} \oplus f_2\mathbb{Z} \oplus \cdots \oplus f_m\mathbb{Z}$$

and

$$N = u_1\mathbb{Z} \oplus u_2\mathbb{Z} \oplus \cdots \oplus u_n\mathbb{Z}.$$

But proposition 2.7 tells us we have  $u_i = d_i f_i$ , for natural numbers  $d_i$  that satisfy  $d_i \mid d_{i+1}$  for  $1 \leq i < n$ . It thus follows that

$$N = d_1 f_1\mathbb{Z} \oplus d_2 f_2\mathbb{Z} \oplus \cdots \oplus d_n f_n\mathbb{Z}.$$

Now consider the quotient group  $F/N$ . It follows immediately that

$$F/N = \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z} \left( \bigoplus_{i=n+1}^m \mathbb{Z}f_i \right).$$

If  $L = \bigoplus_{i=n+1}^m \mathbb{Z}f_i$ , then we have

$$F/N = \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z} (\oplus L)$$

Hence we see that  $G$  is the direct sum of cyclic groups and a free abelian group, as required. The proof is complete.  $\square$

## References

- [1] M. Artin, *Algebra*, Prentice Hall. (1991), 450–475.
- [2] P.Samuel, *Algebraic Theory of Numbers*, Dover. (1970), 19–23.