Classification of Finitely Generated Abelian Groups

The proof given below uses vector space techniques (Smith Normal Form) and generalizes from abelian groups to "modules over PIDs" (essentially generalized vector spaces). Smith Normal Form is a reduced form similar to the row reduced matrices encountered in elementary linear algebra. It is used in number theory to solve systems of linear diophantine (integer!) equations much like row reduced matrices are used to solve linear systems in elementary linear algebra.

Definition: An abelian group G is *finitely generated* if there are a finite number of elements g_1, ..., g_n called *generators* which generate G:

$$G = \langle g_1, \ldots, g_n \rangle = \mathbf{Z}g_1 + \cdots + \mathbf{Z}g_n.$$

In this case $\mathbf{Z}^n = \mathbf{Z} \oplus \cdots \oplus \mathbf{Z} \longrightarrow G$ defined by $(i_1, \ldots, i_n) \mapsto i_1 g_1 + \cdots + i_n g_n$ is an onto homomorphism. Conversely, if there is an onto homomorphism of this type then G is finitely generated.

Let K be the kernel of the homomorphism. Then by the First Isomorphism Theorem, $\mathbf{Z}^n/K \cong G$. Since we wish to determine G, determining the form of subgroups K of $\mathbf{Z}^n$ must be useful. Now $\mathbf{Z}^n$ is isomorphic to itself in many ways. For example, there is an automorphism of $\mathbf{Z}^2$, also called a change of generators, which takes generators $(1,1)$ and $(0,1)$ to $(1,0)$ and $(0,1)$, respectively. Under this automorphism the subgroup $K = \{\, (2i, 2i) \mid i \in \mathbf{Z} \,\}$ becomes subgroup $L = 2\mathbf{Z} \oplus \{0\}$. L is preferable to K, since we see immediately that $\mathbf{Z}^2/K \cong \mathbf{Z}^2/L \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}$.

We will show, by changing generators of $\mathbf{Z}^n$, that $K \cong d_1\mathbf{Z} \oplus \cdots \oplus d_r\mathbf{Z}$ where $d_i | d_{i+1}$, $d_i > 0$, so $G \cong \mathbf{Z}^n/K \cong \mathbf{Z}/d_1\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/d_r\mathbf{Z} \oplus \mathbf{Z} \oplus \cdots \oplus \mathbf{Z}$. First we need a technical result.

Proposition: Every subgroup of $\mathbf{Z}^n$ is finitely generated (by at most n generators).

Proof: Induct on n. Let K be a subgroup. Let F be the first components of elements of K, that is, $f \in F$ if $(f, a_2, \ldots, a_n) \in K$ for some a_i's. F is clearly a subgroup of $\mathbf{Z}$. Pick the least positive element f in F or pick $f = 0$ if F is trivial, and select $(f, a_2, \ldots, a_n) \in K$. Given $(k_1, \ldots, k_n) \in K$ since f is least, by the division algorithm $k_1 = sf$ for some s so

$$(k_1, \ldots, k_n) = s(f, a_2, \ldots, a_n) + (0, k_2 - sa_2, \ldots, k_n - sa_n).$$

The collection of all elements $(k_2 - sa_2, \ldots, k_n - sa_n)$ is a subgroup K' of $\mathbf{Z}^{n-1}$. K' is finitely generated by induction. This shows K is finitely generated. ∎

Theorem: Let K be a subgroup of $\mathbf{Z}^n$. Then $K \cong d_1\mathbf{Z} \oplus \cdots \oplus d_r\mathbf{Z}$ for some $d_i | d_{i+1}$, $d_i > 0$, and $\mathbf{Z}^n/K \cong \mathbf{Z}/d_1\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/d_r\mathbf{Z} \oplus \mathbf{Z} \oplus \cdots \oplus \mathbf{Z}$.

Proof: K is a finitely generated subgroup of $\mathbf{Z}^n$ by the previous proposition. Let k_1, ..., k_m be generators for K and write $k_i = (k_{i1}, \ldots, k_{in})$. Set

$$A = \begin{pmatrix} k_{11} & \ldots & k_{1n} \\ \vdots & \vdots & \vdots \\ k_{m1} & \ldots & k_{mn} \end{pmatrix}$$

Apply row and column operations in $\mathbf{Z}$: the allowed operations are to interchange two rows (resp. columns), to multiply a row (resp. column) by -1, and to add one row (resp. column) to a different row (resp. column). Row operations have the effect of replacing one set of generators $k_1, \ldots, k_m$ of K by some other set of generators of K. For example, the add operation that adds the first to the second row replaces the generators by k_1, $k_2 + k_1$, $k_3, \ldots, k_m$, which are also generators of K. Column operations are similar, except they replace generators of $\mathbf{Z}^n$ by other generators of $\mathbf{Z}^n$.

As described below, by using these row and column operations the integral matrix A can be reduced to *Smith Normal Form*:

$$S = \begin{pmatrix} d_1 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & d_r & 0 & \ldots & 0 \\ 0 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & 0 & \ldots & 0 \end{pmatrix}$$

which proves the result. ∎

Corollary (Classification Theorem for Finitely Generated Abelian Groups): Let G be a finitely generated abelian group. Then $G \cong \mathbf{Z}/d_1\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/d_r\mathbf{Z} \oplus \mathbf{Z} \oplus \cdots \oplus \mathbf{Z}$ for some $d_i | d_{i+1}$, $d_i > 0$.

Proof: Let $g_1, \ldots, g_n$ be generators of G. Consider the homomorphism $\mathbf{Z}^n \longrightarrow G$ defined by $(i_1, \ldots, i_n) \mapsto i_1 g_1 + \cdots + i_n g_n$. By the First Isomorphism Theorem $G \cong \mathbf{Z}^n/K$ where K is the kernel of the homomorphism. Now use the previous theorem. ∎

Computing Smith Normal Form: By induction it suffices to show every integral A can be reduced using integer row and column operations to $\begin{pmatrix} d & 0 \\ 0 & B \end{pmatrix}$ where d divides every entry of B.

Call the absolute value of a non-zero element the *size* of the element and call the upper left entry the pivot. Assume the matrix is non-zero. By interchanging rows or columns move the non-zero element of least size to the pivot. In what follows, whenever we encounter an element in A which is smaller in size than the pivot, we move that element to the pivot; we never increase the size of the pivot. Note that since the elements are integers, this means the pivot will only be changed a finite number of times.

Step 1: Repeatedly add or subtract the pivot from other entries in the first row and in the first column, reducing the size of those entries. The entries either become zero or are smaller in size than the pivot. Since the size can not be reduced indefinitely, at some stage all entries in the first row and first column except the pivot are zero.

Step 2: If the pivot does not divide every element of B, say it does not divide the 2,2 element, then add the second row to the first, and then add or subtract the pivot a sufficient number of times to make the 1,2 element of smaller size than the pivot. Return to Step 1 with this element as pivot. Since the pivot can be reduced in size only a finite number of times, ultimately the pivot will divide every entry of B.