# Abelian Groups-II

We want to re-do the stucture theorem on finitely generated abelian groups using matrices. This will allow us to generalise this theorem to other rings.

For an abelian group $M$, a homomorphism $\mathbb{Z} \to M$ is determined by the image $a$ of 1. More generally, given $a_1$, …, $a_r$ in $M$, we get a homomorphism

$$\mathbb{Z} \times \cdots \times \mathbb{Z} \text{ ($r$ copies) } \to M$$

given by

$$(n_1, \ldots, n_r) \mapsto n_1 \cdot a_1 + \cdots + n_r \cdot a_r$$

Since $\mathbb{Z} \times \cdots \times \mathbb{Z}$ will occur frequently in what follows we use the notation $\mathbb{Z}^r$ for the product of $r$ copies of $\mathbb{Z}$.

In summary, giving a homomorphism $\mathbb{Z}^r \to M$ is the same as giving $r$ elements of $M$.

If $M$ has only finitely many elements (i.e. $M$ is a finite abelian group) then we can take *all* the elements of $M$ and so we have $\mathbb{Z}^r \to M$ is onto $M$ for some suitable $r$.

**Definition**: An abelian group is said to be *finitely generated* if there is an onto homomorphism $\mathbb{Z}^r \to$M$.

**Exercise**: If there is an onto homomorphism $\mathbb{Z}^r \to M$, then there are elements $a_1$,…,$a_r$ so that every element of $M$ can be written as an additive combination of the elements $a_i$. (Note that by convention additive combinations allow subtraction also!)

Note that a finitely generated group *need not* be finite. For example $\mathbb{Z}^r$ is finitely generated (use the identity homomorphism!).

## Projections and Free Abelian Groups

Given an abelian group $M$ and an idempotent $p$ in $\mathrm{End}(M)$; i.e. $p : M \to M$ is an endomorphism such that $p \circ p = p$.

Let $N = \ker(p) = \{a \in M : p(a) = 0\}$ be the kernel of $p$ and $L = p(M)$ be the image of $p$. We have a natural group homomorphism $N \times L \to M$ given by $(n, l) \mapsto n + l$. Given any $a$ in $M$ we can put $l = p(a)$ and $n = a - p(a)$.

**Exercise**: Check that $p(n) = 0$. Moreover, check that if $p(a)$ is in $N$, then $p(a) = 0$ so that $N \cap L = 0$.

**Exercise**: Conclude that $N \times L \to M$ is an isomorphism (i.e. it is one-to-one and onto).

Thinking of $M$ *as* $N \times L$, the map $p : M \to L$ can be thought of as a projection onto the subgroup $L$ of $M$. For this reason, idempotents are sometimes also called *projectors*.

Now suppose that we have a group homomorphism $f : M \to \mathbb{Z}^r$ for some $r$ and that this map is *onto*. For each $i$ between 1 and $r$ we have the element $e_i$ of $\mathbb{Z}^r$ which has 1 in the $i$-th place and 0 elsewhere. Since $f$ is onto, there is an element $a_i$ of $M$ such that $f(a_i) = e_i$.

By the previous discussion, we can define a homomorphism $g : \mathbb{Z}^r \to M$ so that $g(e_i) = a_i$. Moreover, it is obvious that $(f \circ g)(e_i) = f(g(e_i)) = e_i$.

**Exercise**: Show that $f \circ g$ is the identity endomorphism of $\mathbb{Z}^r$.

**Exercise**: Show that $g$ is one-to-one so that $g(\mathbb{Z}^r)$ can be thought of as a copy of $\mathbb{Z}^r$ inside $M$.

**Exercise**: Show that $p = g \circ f$ is an idempotent endomorphism of $M$.

**Exercise**: Show that $M$ is isomorphic to $\ker(f) \times \mathbb{Z}^r$.

In summary, whenver we have an homomorphism of a group $M$ *onto* a free abelian group $\mathbb{Z}^r$, the group $M$ *splits* into a copy of $\mathbb{Z}^r$ and the kernel of the homomorphism.

This important property of free abelian groups is generalised in the notion of "projective modules" which will be introduced later.

## Subgroups of Free Abelian Groups

Let $L$ denote a subgroup of the free abelian group $\mathbb{Z}^r$. We will prove by induction on $r$ that $L$ is isomorphic to a free abelian group $\mathbb{Z}^s$ for some non-negative integer $s \leq r$.

The starting point is the fact that a subgroup of $\mathbb{Z}$ is of the form $\mathbb{Z} \cdot n$; i.e. it consists of all multiples of some non-negative integer $n$. This proves the result for $r = 1$.

Moreover, if $r > 1$, then we can take $L \cap (\mathbb{Z} \cdot e_1)$ which is a subgroup of $\mathbb{Z} \cdot e_1$ and hence is of the form $\mathbb{Z} \cdot (n \cdot e_1)$ for some non-negative integer $n$.

Now, the group $L/(L \cap (\mathbb{Z} \cdot e_1))$ is a subgroup of $\mathbb{Z}^r/\mathbb{Z} \cdot e_1$. The latter is clearly isomorphic to the free abelian group $\mathbb{Z}^{r-1}$. By induction on $r$ it is isomorphic to $\mathbb{Z}^t$ for some $t \leq r - 1$.

Thus, $L$ has an onto homomorphism onto the free abelian group $\mathbb{Z}^t$ with kernel of the form $\mathbb{Z} \cdot (n \cdot e_1)$. By the results of the previous sub-section, this means that $L$ is of the form $\mathbb{Z} \cdot (n \cdot e_1) \times \mathbb{Z}^t$. If $n = 0$, then this is the same as $\mathbb{Z}^t$. On the other hand, if $n \neq 0$ then $\mathbb{Z} \cdot (n \cdot e_1)$ is isomorphic to $\mathbb{Z}$, since no multiple of $n \cdot e_1$ becomes 0; in this case $L$ becomes isomorphic to $\mathbb{Z}^{t+1}$. Since $t < t + 1 \leq r$, we have proved the inductive step.

## Finitely Generated Abelian Groups and Matrices

For a finitely generated abelian group $M$, we have an onto homomorphism $f : \mathbb{Z}^r \to M$. The kernel of $f$ is a subgroup of $\mathbb{Z}^r$. So as seen above it is isomorphic to $\mathbb{Z}^s$.

The basis element $f_i$ of $\mathbb{Z}^s$ is mapped to an element $a_i$ of $\mathbb{Z}^r$ under this isomorphism. Writing $a_i$ as a column (integer) vector with $r$ rows, we see that the the kernel of $f$ is the image of $\mathbb{Z}^s$ by an $r \times s$ matrix $A$ with integer entries; the $i$-th column of $A$ is $a_i$. A column (integer) vector $v$ with $s$ rows is sent to $A \cdot v$ under this homomorphism. Note that since $s \leq r$ we can "pad" the matrix with 0 columns to make $A$ a square $r \times r$ matrix.

In summary, any finitely generated group is isomorphic to a group of the form $\mathbb{Z}^r / A \cdot \mathbb{Z}^r$ for some $r \times r$ integer matrix $A$. The study of finitely generated groups can be thus reduced to the study of such matrices.

If $e_i$ for $i = 1, \ldots, r$ denote the standard generators of $\mathbb{Z}^r$, then we have another system of generators $f_i$ for $i = 1, \ldots, r$ where $f_i = e_i$ for $i \neq k$ and $f_k = e_k + n \cdot e_j$ for some integer $n$ and some index $j$. Similarly, we can obtain another system of generators by permuting the original system of generators. This change of generators will not change the isomorphism class of the quotient group. These changes correspond to row and column operations on the matrix $A$ of the following type:

- Add an integer multiple of the $j$-th row to the $k$-th row.
- Add an integer multiple of the $j$-th column to the $k$-th column.
- Swap two rows.
- Swap two columns.

Thus, if we want to understand finitely generated abelian groups upto isomorphism, it is acceptable to try to "reduce" or simplify the matrix $A$ using these operations.

The basic steps of the first reduction are as follows.

1. Locate the smallest (in absolute value) non-zero entry in $A$; suppose it is $a$ which is in the $k$-th row and $\ell$-th column of $A$.

2. Given any other non-zero entry in the same row, say it is $b$ which is in the $j$-th column. We will then write $b = q \cdot a + r$ where $0 \leq r < |a|$ by using integer division.

3. We then subtract $q$ times the $\ell$-th column from the $j$-th column. This will replace the entry $b$ in the $k$-row and $j$-th column by $r$ which is less than $|a|$ or it is zero.

4. We repeat the above steps 2 and 3 with all non-zero entries in the $k$-row.

5. We do identical operations as 2, 3 and 4 with columns instead instead of rows for all non-zero entries in the $\ell$-th column.

6. Either we made some "new" small entries (if some remainder is non-zero) and then we go back to step 1, or *all* entries in the $k$-th row other than the given one are 0. Similarly, for *all entries in the $\ell$-th column.

7. We now swap this row with the last row and this column with the last column and "fix" it. We then continue to perform reduction on the submatrix of all the remaining rows and columns.

As a result of this reduction we obtain a matrix $D$ all of whose non-zero entries *must* lie on the diagonal. Note that $\mathbb{Z}^r/D \cdot \mathbb{Z}^r$ is of the form

$$\mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_r$$

Here $d_i$ are the diagonal entries of $D$. Of course, we should note that $\mathbb{Z}/1$ is the group $\{0\}$ which consists of a single element and that the group $\mathbb{Z}/0$ is the same as $\mathbb{Z}$.

Can we do better than this? To understand how we can, let us take an example. Start with the matrix $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$. We perform the following steps:

- Add row 1 to row 2. So $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \mapsto \begin{pmatrix} 2 & 0 \\ 2 & 3 \end{pmatrix}$
- Subtract column 1 from column 2. So $\begin{pmatrix} 2 & 0 \\ 2 & 3 \end{pmatrix} \mapsto \begin{pmatrix} 2 & -2 \\ 2 & 1 \end{pmatrix}$
- Subtract 2 times column 2 from column 1. So $\begin{pmatrix} 2 & -2 \\ 2 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 6 & -2 \\ 0 & 1 \end{pmatrix}$
- Add 2 times row 2 to row 1. So $\begin{pmatrix} 6 & -2 \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 6 & 0 \\ 0 & 1 \end{pmatrix}$
- Finally we can swap both rows and both columns $\begin{pmatrix} 6 & 0 \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$

This is "simpler" than the original since $d_1$ divides $d_2$!

It is reasonably clear that if we operate on entries of $D$ pair-wise, we can use these steps to make the diagonal entries of $D$ satisfy $d_1|d_2|\cdot|d_r$. Note that some of the initial $d_i$'s could be 1 and some of the last $d_i$'s could be 0. No further reduction is possible after this!

As a consequence, we obtain the structure theorem of finitely generated abelian groups.

**Theorem**: A finitely generated abelian group is isomorphic to

$$(\mathbb{Z}/n_1) \times (\mathbb{Z}/n_2) \times \cdots \times (\mathbb{Z}/n_p) \times \mathbb{Z}^q$$

where $n_1$ divides $n_2$, and so on upto $n_p$ are positive integers. Moreover, these numbers and the non-negative integer $q$ uniquely determine the finitely generated abelian group upto isomorphism.