

The Structure Theorem for Finitely Presented Abelian Groups

In the previous handout, we explained the mechanics of the Smith Normal Form algorithm. In this handout, we discuss in more detail how that algorithm is applied to find the structure of finitely presented abelian groups.

If S is a set, the *free abelian group on S* , denoted by \mathbb{Z}^S , is the set of all linear combinations $\sum_{s \in S} a_s s$ with $a_s \in \mathbb{Z}$, where we restrict to combinations for which $a_s = 0$ for all but finitely many $s \in S$. The group law is

$$\left(\sum_{s \in S} a_s s\right) + \left(\sum_{s \in S} b_s s\right) = \sum_{s \in S} (a_s + b_s) s.$$

A group G is *finitely generated* if there is an epimorphism $\pi : \mathbb{Z}^S \rightarrow G$ for some finite set S . If the kernel of π is also finitely generated, we say that G is *finitely presented*. It is not hard to see that any finite group is finitely presented.

For a finitely presented group, there is a homomorphism $\rho : \mathbb{Z}^T \rightarrow \mathbb{Z}^S$ for some finite sets S and T , such that the image of ρ is the kernel of π . Thus, the original group G is isomorphic to the *cokernel* of ρ :

$$G \cong \mathbb{Z}^S / \text{im } \rho.$$

There may be many different generating sets for G and for $\ker \pi$. We will restrict our attention to changes of generating sets for \mathbb{Z}^S and \mathbb{Z}^T (where we take the sets S and T to be finite). If $\mathbb{Z}^S \cong \mathbb{Z}^{S'}$ for two sets $S = \{s_1, \dots, s_m\}$ and $S' = \{s'_1, \dots, s'_m\}$ of the same cardinality, then there must be expressions

$$s_j = \sum s'_i \sigma_{ij}, \quad s'_\ell = \sum s_k \sigma'_{k\ell}$$

which can be summarized by two square matrices Σ and Σ' with integer entries; by definition, we have

$$s_j = \sum s'_i \sigma_{ij} = \sum s_k \sigma'_{ki} \sigma_{ij}$$

so $\Sigma' \Sigma = I_m$, the $m \times m$ identity matrix. Similarly, $\Sigma \Sigma' = I_m$. In other words, *changing the generating set for \mathbb{Z}^S is accomplished via an invertible $m \times m$ matrix over the integers.*

Similarly, changing the generating set for \mathbb{Z}^T is accomplished via an invertible $n \times n$ matrix over the integers.

If we have chosen generating sets $S = \{s_1, \dots, s_m\}$ and $T = \{t_1, \dots, t_n\}$, then the homomorphism ρ can be described by means of its action on the generators: we can write

$$\rho(t_j) = \sum_1 s_i r_{ij}$$

for some matrix of integers $R = (r_{ij})$ which characterized ρ with respect to those generating sets. On the other hand, if Σ and Ξ describe changes of generating set, then

$$\Xi R \Sigma$$

is the matrix describing ρ with respect to the new generating sets. This is the type of change which was analyzed in our discussion of the Smith normal form.

As a consequence, the Smith normal form algorithm guarantees us that given a finitely presented group G , there exist generating sets for \mathbb{Z}^S and \mathbb{Z}^T such that the matrix for ρ is in diagonal form, with diagonal entries a_i such that a_i divides a_{i+1} . If s'_1, \dots, s'_m are the appropriate generators, this then tells us that $a_1 s'_1, \dots, a_m s'_m$ are the relations (with all relations being given as linear combinations of those). Thus, G is isomorphic to

$$\mathbb{Z}_{|a_1|} \oplus \cdots \oplus \mathbb{Z}_{|a_m|},$$

where \mathbb{Z}_0 denotes \mathbb{Z} itself.

The structure theorem for finite abelian groups has one additional ingredient: the uniqueness of the cyclic factors. This can be verified by a careful count of how many elements there are of each order in a direct sum of cyclic groups.