Background material: Finitely generated abelian groups

This term we will be working with vector spaces and abelian groups. Thinking of abelian groups as "vectors spaces over $\mathbb{Z}$" – correctly as "modules over $\mathbb{Z}$" – much of the theory of vector spaces has an analogue for abelian groups.

Let $L : \mathbb{Z}^n \to \mathbb{Z}^m$ be a group homomorphism. Then with respect to a chosen basis (i.e. a set of n respectively m generators) of $\mathbb{Z}^n$ and $\mathbb{Z}^m$, L can be represented as a matrix $M = (m_{ij})$ of integers.

An integer matrix is *invertible over* $\mathbb{Z}$ if its inverse has integer entries. Changing the matrix by such an over $\mathbb{Z}$ invertible row operation corresponds to changing the basis of $\mathbb{Z}^m$, the target; changing it by an over $\mathbb{Z}$ invertible column operation corresponds to changing the basis of $\mathbb{Z}^n$, the source.

Theorem (Smith Normal Form). *Let L be a matrix with entries in $\mathbb{Z}$ and m rows and n columns. Then there are square matrices P and Q, invertible over $\mathbb{Z}$, such that*

$$PLQ = \begin{pmatrix} d_1 & 0 & 0 & \dots \\ 0 & d_2 & 0 & \dots \\ 0 & 0 & d_3 & \dots \\ 0 & 0 & 0 & \dots \end{pmatrix}.$$

Furthermore, this can be done such that $d_1 | d_2, d_2 | d_3, \dots$.

One of the most important applications of this theorem is the classification of finitely generated abelian groups.

Theorem (Classification of f.g. abelian groups). *Let M be a finitely generated abelian group. Then M is isomorphic to the direct product of cyclic groups*

$$M \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_t\mathbb{Z}.$$

Again, it can be arranged such that $d_1 | d_2, d_2 | d_3, \dots$.

Note that if $d_i = 1$ then the corresponding factor is zero; if $d_i = 0$ then the corresponding factor is free, i.e. $\mathbb{Z}$. In particular every finitely generated abelian group can be written as

$$M = T \oplus F$$

where T is the subgroup of all torsion elements of M and F is free abelian, i.e. $F \simeq \mathbb{Z}^k$ for some k.