MAT301: Extra Topics

QiLin Xue

August 9, 2021

Contents

Free Abelian Group

The notion of a free abelian group is important. While during class this was introduced as a tool to solve another problem (classification of finitely generated abelian groups), I will introduce it first to prevent the flow from being broken up in the next section.

Before we define free abelian groups, we need to make a connection between abelian groups and linear algebra.

■ Relationship between Abelian Groups and Vector Spaces

In this section, we make the connection between free abelian groups and vector spaces. The fact that the group operator of abelian groups is typically written as addition $+$ is suggestive of this relationship.

Specifically, just like how vectors can span a vector space, a linear combination of elements can span a group. For formality, we introduce the following definitions:

> **Definition Set of $\mathbb{Z}$ linear combinations of elements of S**
> Let $(A, +)$ be an abelian group. Note that if $S \subseteq A$, then
>
> $$\langle S \rangle = \left\{ \sum_{i=1}^{m} k_i a_i : m \in \mathbb{Z}_{\geq 0},\, a_i \in S, k_i \in \mathbb{Z} \right\}$$
>
> where the right hand side can be denoted as span$_{\mathbb{Z}}(S)$, which is the set of all $\mathbb{Z}$ linear combinations of elements of S.

Since empty sets are trivial, we have

$$\text{span}_{\mathbb{Z}}(\emptyset) = \{0\}$$

> **Definition Linear Independence, Span, Basis**
> Let $S \subseteq A$.
>
> 1. S is linearly independent (over $\mathbb{Z}$) if for any $m \in \mathbb{Z}_{>0}$, $a_1, \ldots, a_m \in S$, and $k_1, \ldots, k_m \in \mathbb{Z}$,
>
> $$\sum_{i=1}^{m} k_i a_i = 0 \implies a_1 = \cdots = a_m = 0,$$
>
>   or equivalently if every element of A can be written as a $\mathbb{Z}$-linear combination of elements of S in at most one way.
> 2. S spans A (over $\mathbb{Z}$) if $A = \mathrm{span}_{\mathbb{Z}}(S)$, or equivalently every element of A can be written as a $\mathbb{Z}$-linear combination of elements of A in at least one way.
> 3. S is a basis (or $\mathbb{Z}$-basis) of A if S is linearly independent and spans A, or equivalently if every element of A can be written as a $\mathbb{Z}$-linear combination of elements of S in exactly one way.

■ **Example 1:** $e_1, \ldots, e_m$ is a basis of $\mathbb{Z}^m$.

■ Definition of Free Abelian Group

> **Definition Free Abelian Group**
> A free abelian group is an abelian group that has a basis.
>
> A free abelian group of finite rank is an abelian group that has a finite basis.

■ **Example 2:** $\mathbb{Z}^m$ is a free abelian group of finite rank for all $m \in \mathbb{Z}_{\geq 0}$. Note that $\mathbb{Z}^0 = \{0\}$.

■ **Example 3:** If $\{v_1, \dots, v_m\} \subseteq \mathbb{R}^n$ is linearly independent over $\mathbb{R}$ and A is the subgroup of $\mathbb{R}^n$ generated by $\{v_1, \dots, v_n\}$, i.e. $A = \langle v_1, \dots, v_n \rangle = \operatorname{span}_{\mathbb{Z}}(\{v_1, \dots, v_n\})$, then $\{v_1, \dots, v_n\}$ is a $\mathbb{Z}$-basis of A, so A is a free abelian group of finite rank.

■ **Example 4:** If $\{G_i\}_{i\in I}$ is a set of abelian groups, then

$$\bigoplus_{i\in I} G_i := \left\{ (g_i)_{i\in I} \in \prod_{i\in I} G_i \,\middle|\, g_i = e_{G_i} \text{ for all but finitely many } i \in I \right\}$$

is a subgroup of the direct product $\prod_{i\in I} G_i$. Note that we can call $\bigoplus_{i\in I} G_i$ the direct sum of $\{G_i\}_{i\in I}$.

If I is infinite and $G_i = \mathbb{Z}$ for all $i \in I$, then $\bigoplus_{i\in I} G_i = \bigoplus_{i\in I} \mathbb{Z}$ is a free abelian group that is not of finite rank (it has an infinite basis but no finite basis).

Note that free abelian groups are like vector spaces over $\mathbb{Z}$.

■ Properties of Free Abelian Groups

■ Proposition 1.1: Relationship to $\mathbb{Z}^m$

A group is a free abelian group of finite rank if and only if it is isomorphic to $\mathbb{Z}^m$ for some $m \in \mathbb{Z}_{\geq 0}$.

Proof: Let A be a group. If $m \in \mathbb{Z}_{\geq 0}$ and $\phi : \mathbb{Z}^m \to A$ is an isomorphism, then $\{\phi(e_1), \cdots, \phi(e_m)\}$ is a basis of A.

Conversely, if A is a free abelian group of finite rank and $\{a_1, \dots, a_n\}$ is a basis of A, then

$$\begin{aligned} \phi : \mathbb{Z}^m &\to A \\ (k_1, \dots, k_m) &\mapsto k_1 a_1 + \cdots + k_m a_m \end{aligned}$$

is an isomorphism. ■

■ Proposition 1.2: Cardinality of Rank

Let A be a free abelian group of finite rank. then all bases of A have the same cardinality.

Proof: Let $\{a_1, \dots, a_m\}$ be a basis of A.

Let $\{a'_j\}_{j\in J}$ be a basis of A. For each $i = 1, \dots, m$, there exists a finite subset $S_i \subseteq \{a'_j\}_{j\in J}$ such that a_i is a linear combination of the elements of S_i. Let $S = S_1 \cup \cdots \cup S_m$.

Then $a_1, \dots, a_m$ are all linear combinations of the elements of S. Since $\{a_1, \dots, a_m\}$ spans A, it follows that every element of A is a linear combination of the elements of S, i.e. S spans A. Let $a_{j_1}, \dots, a_{j_n}$ be the elements of S.

Suppose for a contradiction that $\{a'_j\}_{j\in J}$ is infinite. Then there exists $j \in J$ such that $a'_j \neq a_j, \dots, a'_{j_n}$. There exist $k_1, \dots, j_n \in \mathbb{Z}$ such that

$$a'_j = \sum_{i=1}^{n} k_i a'_{j_i}, \tag{1}$$

but this contradicts linearly independence of $\{a'_j\}_{j\in J}$.

Therefore $\{a'_j\}_{j\in J}$ is finite. Let $a'_1, \dots, a'_n$ be the elements of $\{a'_j\}_{j\in J}$. Since $\{a_1, \dots, a_m\}$ spans A, for all $i = 1, \dots, n$ we can write

$$a'_i = \sum_{j=1}^{m} M_{ij} a_j \tag{2}$$

for some $M_{i1}, \dots, M_{im} \in \mathbb{Z}$.

Similarly, since $\{a'_1, \ldots, a'_n\}$ spans A, for all $i = 1, \ldots, m$ we can write

$$a_i = \sum_{j=1}^{n} N_{ij} a'_j \tag{3}$$

for some $N_{i1}, \ldots, N_{in} \in \mathbb{Z}$.

For all $i = 1, \ldots, n$, we have

$$\begin{aligned} a'_i &= \sum_{j=1}^{m} M_{ij} a_j \\ &= \sum_{j=1}^{m} M_{ij} \sum_{k=1}^{n} N_{jk} a'_k \\ &= \sum_{j=1}^{m} \sum_{k=1}^{n} M_{ij} N_{jk} a'_k \\ &= \sum_{k=1}^{n} \sum_{j=1}^{m} M_{ij} N_{jk} a'_k \\ &= \sum_{k=1}^{n} \left(\sum_{j=1}^{m} M_{ij} N_{jk} \right) a'_k \end{aligned}$$

Since $\{a'_1, \ldots, a'_n\}$ is linearly independent, it follows that

$$\left(\sum_{j=1}^{m} M_{ij} N_{jk} \right) = \delta_{ik} \tag{4}$$

for all $i, k = 1, \ldots, n$.

Similarly, for all $i, k = 1, \ldots, m$ we have

$$\sum_{j=1}^{n} N_{ij} M_{jk} = \delta_{ik}. \tag{5}$$

Let $M = [M_{ij}] \in \mathsf{Mat}_{n \times m}(\mathbb{Z})$ and $N = [N_{ij}] \in \mathsf{Mat}_{m \times n}(\mathbb{Z})$.

Then $MN = I_n$ and $NM = I_m$. Therefore, the $\mathbb{Q}$-linear transformations

$$\begin{aligned} \mathbb{Q}^m &\to \mathbb{Q}^n \\ x &\mapsto Mx \end{aligned}$$

and

$$\begin{aligned} \mathbb{Q}^n &\to \mathbb{Q}^m \\ x &\mapsto Nx \end{aligned}$$

are inverses of each other. Therefore $\mathbb{Q}^m$ and $\mathbb{Q}^n$ are isomorphic vector spaces over $\mathbb{Q}$, so $m = n$. ■

■ Definition of Rank

Therefore, we can remove the assumption that A is of finite rank from the proposition. This also introduces the notion of a rank:

> **Definition Rank of a Free Abelian Group**
> Let A be a free abelian group. The rank of A is the cardinality of some (and hence any) basis of A and is denoted by $\operatorname{rank}(A)$.

■ Proposition 1.3: Finite groups have finite ranks

Let A be a finitely generated group. Then A is of finite rank if and only if A is a finite group.

Proof: The "only if" direction is immediate. Suppose A is a finite group and let $\{g_1, \ldots, g_m\}$ be a generating set of A. Let $\{a_i\}_{i \in I}$ be a basis of A. There is a finite subset $\{a_{i_1}, \ldots, a_{i_n}\}$ of $\{a_i\}_{i \in I}$ such that

$$\{g_1, \ldots, g_m\} \subseteq \operatorname{span}_{\mathbb{Z}} \left(\{a_{i_1}, \ldots, a_{i_n}\}\right).$$

Then

$$A = \operatorname{span}_{\mathbb{Z}}(\{g_1, \ldots, g_m\}) \subseteq \operatorname{span}_{\mathbb{Z}} \left(\{a_{i_1}, \ldots, a_{i_n}\}\right) \subseteq A,$$

so $\operatorname{span}_{\mathbb{Z}} \left(\{a_{i_1}, \ldots, a_{i_n}\}\right) = A$. Since $\{a_{i_1}, \ldots, a_{i_n}\} \subseteq \{a_i\}_{i \in I}$ and $\{a_i\}_{i \in I}$ us linearly independent, it follows that $\{a_{i_1}, \ldots, a_{i_n}\}$ is linearly independent. Therefore, $\{a_{i_1}, \ldots, a_{i_n}\}$ is a basis of A, so A is of finite rank. ■

Warning! Here are a few misconceptions. Take $\mathbb{Z}$ for example. THen:

- $\{2, 3\}$ is a minimal spanning subset of $\mathbb{Z}$, but it is not a basis as it is linearly dependent.
- $\{2, 3\}$ spans $\mathbb{Z}$, but does not contain a basis of $\mathbb{Z}$.
- $\{2\}$ is a maximal linearly independent subset of $\mathbb{Z}$, but it is not a basis because its span is $2\mathbb{Z} \subsetneq \mathbb{Z}$.
- $\{2\}$ is linearly independent, but it is not contained in a basis of $\mathbb{Z}$.

Homomorphisms of Free Abelian Groups

Proposition 1.4: Homomorphisms and Bases

Let A be a free abelian group and let $\{a_i\}_{i \in I}$ be a basis of A.

Let B be an abelian group and let $\{b_i\}_{i \in I}$ be a family of elements of B.

Then there exists a unique homomorphism $\phi : A \to B$ such that $\phi(a_i) = b_i$ for all $i \in I$. It is surjective if and only if $\{b_i\}_{i \in I}$ spans B, it is injective if and only if $\{b_i\}_{i \in I}$ is linearly independent, and it is an isomorphism iff $\{b_i\}_{i \in I}$ is a basis of B.

Let A be a free abelian group of finite rank n. For any basis $\alpha = \{a_1, \ldots, a_n\}$ of A there exists a unique isomorphism:

$$\theta_\alpha : A \to \mathbb{Z}^n$$

such that $\theta(a_i) = e_i$ for all $i = 1, \ldots, n$. Note that:

- $\theta_\alpha^{-1}(k_1, \ldots, k_n) = \displaystyle\sum_{i=1}^{n} k_i a_i$
- For all $a \in A$, let us write $[a]_\alpha = \theta_\alpha(a) \in \mathbb{Z}^n$.

Proposition 1.5: Matrices and Homomorphisms

Let A, B be free abelian groups of finite ranks n and m, respectively. Let $\alpha = \{a_1, \ldots, a_n\}$ be a basis of A and $\beta = \{b_1, \ldots, b_m\}$ be a basis of B. For all homomorphisms $\phi : A \to B$ there exists a unique matrix

$$[T]^\alpha_\beta \in \mathsf{Mat}_{m \times n}(\mathbb{Z})$$

such that for all $a \in A$ we have

$$[Ta]_\beta = [T]^\alpha_\beta [a]_\alpha.$$

Let C be a free abelian group of finite rank p and let $\gamma = \{c_1, \ldots, c_p\}$ be a basis of C. If $T : A \to B$ and $S : B \to C$ are homomorphisms, then

$$[S \circ T]^\alpha_\gamma = [S]^\beta_\gamma [T]^\alpha_\beta$$

Proof: Let $T : A \to B$ be a homomorphism. Define

$$[T]^\alpha_\beta = [[Ta_1]_\beta \cdots [Ta_n]_\beta].$$

The rest is straightforward. ■

In words, this says that we can take any element $a \in A$ to $b \in B$ using the homomorphism T and write it as a vector using the basis of B. This is equivalent to first writing a as a vector using the basis of A, and multiplying it by some matrix $[T]_\beta^\alpha$ that transforms the vector from an α basis to a β basis. Essentially, this is a change of basis matrix.

Corollary

A homomorphism $T : A \to B$ is an isomorphism if and only if there exists $N \in \mathsf{Mat}_{n\times m}(\mathbb{Z})$ such that

$$[T]_\beta^\alpha n = I_m \text{ and } N[T]_\beta^\alpha = I_n$$

in which case $m = n$.

Matrices

As previously seen, we can make connections between free abelian groups and matrices. Here are a few more important theorems which will help later:

Invertible Element of $\mathsf{Mat}_{n\times n}(\mathbb{Z})$

> **Definition Invertible Element of $\mathsf{Mat}_{n\times n}(\mathbb{Z})$**
> Let n be a positive integer and $M \in \mathsf{Mat}_{n\times n}(\mathbb{Z})$. We say that M is an invertible element of $\mathsf{Mat}_{n\times n}(\mathbb{Z})$ if there exists $N \in \mathsf{Mat}_{n\times n}(\mathbb{Z})$ such that
> $$MN = I_n = NM,$$
> in which case N is unique, denoted by M^{-1}, and called the *inverse of M*. We denote the subset of invertible elements of $\mathsf{Mat}_{n\times n}(\mathbb{Z})$ by $\mathsf{GL}_n(\mathbb{Z})$.

Note that $M \in \mathsf{Mat}_{n\times n}(\mathbb{Z})$ is invertible if and only if it is invertible in $\mathsf{Mat}_{n\times n}(\mathbb{Q})$ and $M^{-1} \in \mathsf{Mat}_{n\times n}(\mathbb{Z})$.

Classification of $\mathsf{GL}_n(\mathbb{Z})$

$$\mathsf{GL}_n(\mathbb{Z}) = \{M \in \mathsf{Mat}_{n\times n}(\mathbb{Z}) | \det(M) \in \{\pm 1\}$$

Proof: If $M \in \mathsf{GL}_n(\mathbb{Z})$, then

$$\det(M)\det\left(M^{-1}\right) = \det(I_n) = 1$$

Since $\det(M), \det\left(M^{-1}\right) \in \mathbb{Z}$, it follows that $\det(M) = \det\left(M^{-1}\right) = \pm 1$.

If $M \in \mathsf{Mat}_{n\times n}(\mathbb{Z})$ and $\det(M) = \pm 1$, then the usual formula for $M^{-1} \in \mathsf{Mat}_{n\times n}(\mathbb{Q})$ shows that $M^{-1} \in \mathsf{Mat}_{n\times n}(\mathbb{Z})$. Thus, $M \in \mathsf{GL}_n(\mathbb{Z})$. ■

Proposition 1.6: Ranks of Subgroups

For each free abelian group A of finite rank, every subgroup B of A is a free abelian group and

$$\operatorname{rank} B \leq \operatorname{rank} A$$

Remarks: One can drop the assumption that A is of finite rank.

Proof: We will proceed by induction on $m = \operatorname{rank}(A)$.

If $m \geq 0$ and assume that for each abelian group of rank m, every subgroup of it is a free abelian group of rank at most m.

Let A be a free abelian group of rank $m+1$ and let $B \leq A$. We can choose a basis $\alpha = \{a_1, \ldots, a_{m+1}\}$ of A and define

$$A' = \operatorname{span}_{\mathbb{Z}}(\{a_1, \ldots, a_m\}) \leq A$$

Then A' is a free abelian group of rank m. ■

Theorem: Smith Normal Form

Let $M \in \mathsf{Mat}_{m\times n}(\mathbb{Z})$. There exist a sequence of integral elementary row and column operations that transform M to a matrix of the form

$$\left[\begin{array}{ccc|c} d_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & d_r & \\ \hline & 0 & & 0 \end{array}\right],$$

where $d_1|\cdots|d_n$ are positive integers. Moreover, $r = \operatorname{rank}(M)$ and for all $i = 1, \dots, r$, $d_i = d_i(M)/d_{i-1}(M)$. In particular, $r, d_1, \dots, r_r$ are unique.

> **Definition** i^{th} **determinant divisor of** M
> For $i = 1, \dots, \min\{m, n\}$, define
>
> $$d_i(M) := \gcd\{\text{determinants of } i \times i \text{ minors of } M.\}$$
>
> and define $d_0(M) = 1$. The number $d_i(M)$ is called the i^{th} determinant divisor of M.

Note that if $i < \operatorname{rank}(M)$, then $d_i(M) > 0$.

Integral Elementary Row Operations

There are three main operations:

- To interchange row i and row j, this is equivalent to multiplying on the left by $P_{i,j}$.
- To multiply row i by -1, we multiply on the left by D_i.
- To replace row i with row i plus k times row j, we multiply on the left by $E_{ij}(k)$.

Note that if we were to act on the columns instead, the elementary matrices should be multiplied on the right.

The integral elementary matrices $P_{ij}, D_i, E_{ij}(k)$ generate the group $\mathsf{GL}_n(\mathbb{Z})$.

Smith Normal Form Algorithm

If $M = 0$, we are done. Assume $M \neq 0$.

1. Let $\delta(M) = \min\{|M_{ij}| : M_{ij} \neq 0\}$. Choose $M_{ij} \neq 0$ such that $|M_{ij}| = \delta(M)$.
2. If M_{ij} does not divide an entry in its row, say $M_{i\ell}$, and $M_{i\ell} = gM_{ij} + r$ where $q, r \in \mathbb{Z}$ and $0 < r < |M_{ij}|$, then replace col$_\ell$ with col$_\ell - q$col$_j$:
3. This results in a matrix M' with $M'_{i\ell} = r$ and $\delta(M') \leq r < |M_{ij}| = \delta(M)$. Let M denote M' now. Go to the previous step.
4. If M_{ij} does not divide an entry in its column, we do the same thing analogous to the previous step.
5. If M_{ij} divides every entry in its row and column, we can clear the other entries in row i and column j using M_{ij} (i.e. all the other entries are 0). Let M denote the resulting matrix.
6. If M_{ij} divides every entry in M, skip this step. Otherwise, choose $M_{k\ell}$ such that $M_{ij} \nmid M_{k\ell}$. Then replace row i with row$_i$ + row$_j$. Let M denote the new matrix. Go to the first step.
7. M_{ij} divides every entry of M. Swap row 1 and row i and swap column 1 and column j. If $M_{ij} < 0$, multiply row by -1.

   We look at the resulting matrix M' in the bottom right corner inside the larger matrix. Let M denote M'.
8. Repeat steps 1 to 6 until M' in the previous step is the empty matrix.

Finitely Generated Abelian Groups

■ Definition of Finitely Generated Abelian Groups

Definition Finitely Generated Groups
A group G is finitely generated (FG) if there exists $g_1, \dots, g_n \in G$ such that

$$\begin{aligned} G &= \langle g_1, \dots, g_n \rangle \\ &:= \bigcap_{H \leq G, \quad g_1, \dots, g_n \in H} H \end{aligned}$$

or equivalently, every element of G can be written as the product of integer powers of g_i.

■ **Example 5:** D_n is finitely generated since $D_n = \langle r, s \rangle$

■ **Example 6:** Every cyclic group is finitely generated, so $\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}$ are finitely generated for all $n \in \mathbb{Z}_{\geq 0}$

■ **Example 7:** If $G_1, \dots, G_n$ are finitely generated groups, then so is $G_1 \times \cdots \times G_n$.
Consequently, $\mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$ is a finitely generated abelian group for all $r, n \in \mathbb{Z}_{\geq 0}$ and $d_1, \dots, d_n \in \mathbb{Z}_{>0}$.

■ Classification of Finitely Generated Abelian Groups

Let A be a finitely generated abelian group. Then it can be classified in either of the two (perfectly equivalent) ways:

1. There exists $r, n \in \mathbb{Z}_{\geq 0}$ and positive integers $d_1 | \cdots | d_n$ such that

$$A \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}. \tag{6}$$

   Moreover, $r, n, d_1, \dots, d_n$ are unique and the d_i are called the **invariant factors of** A

2. There exist $r, s \in \mathbb{Z}_{\geq 0}$, prime numbers $p_1 < \cdots < p_s$, positive integers $n_1, \cdots, n_s$, and positive integers

$$\begin{gathered} e_{1,1} \geq \cdots \geq e_{1,n_1} \\ e_{2,1} \geq \cdots \geq e_{2,n_2} \\ \vdots \\ e_{s,1} \geq \cdots \geq e_{s,n_s} \end{gathered}$$

   such that

$$\begin{aligned} A &\cong \mathbb{Z}^r \times \mathbb{Z}/p_1^{e_{1,1}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_1^{e_{1,n_1}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{e_{s,1}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{e_{s,n_s}}\mathbb{Z} \\ &\cong \mathbb{Z}^r \times \prod_{j=1}^{n_1} \mathbb{Z}/p_1^{e_{i,j}}\mathbb{Z} \times \cdots \times \prod_{j=1}^{n_s} \mathbb{Z}/p_s^{e_{s,j}}\mathbb{Z}. \end{aligned}$$

   Moreover, r and s, and the p_i, n_i and $e_{i,j}$ are all unique.

   More concisely, there exist $r, t \in \mathbb{Z}_{>0}$ and prime powers $q_1 \leq \cdots \leq q_t$ such that

$$A \cong \mathbb{Z}^r \times \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_t\mathbb{Z} \tag{7}$$

   and r, t, q_i are unique. Note the q_i are known as the **elementary divisors of** A**.**

Note that A is finite if and only if $r = 0$. Therefore, the theorem specializes to the classification of finite abelian groups. To prove this, we will do the following:

1. Show that an isomorphism as in (1) exists by reducing the problem to a result in linear algebra.
2. We will construct an isomorphism as in (2) from an isomorphism as in (1), and vice versa.

Lemma: Homomorphism from $\mathbb{Z}^m \to A$

Let $(A, +)$ be an abelian group. Then A is finitely generated if and only if there exists $m \in \mathbb{Z}_{>0}$ and a surjective homomorphism $\phi : \mathbb{Z}^m \to A$.

Proof: Suppose that there exist $m \in \mathbb{Z}_{>0}$ and a surjective homomorphism $\phi : \mathbb{Z}^m \to A$.

Let $a \in A$. THen, there exists $(x_1, \ldots, x_m) \in \mathbb{Z}^m$ such that $a = \phi(x_1, \ldots, x_m)$. For $i = 1, \ldots, m$, let

$$e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{Z}^m \tag{8}$$

where the i^{th} entry is a 1. Then $(x_1, \ldots, x_m) = \sum_{i=1}^{m} x_i e_i$. Therefore

$$a = \phi\left(\sum_{i=1}^{m} x_i e_i\right) = \sum_{i=1}^{m} x_i \phi(e_i). \tag{9}$$

Therefore $A = \langle \phi(e_1), \ldots, \phi(e_n) \rangle$, so A is finitely generated.

To show the converse, suppose A is finitely generated and let $a_1, \ldots, a_m \in A$ such that $A = \langle a_1, \ldots, a_m \rangle$. Define

$$\phi : \mathbb{Z}^m \to A \tag{10}$$

by $\phi(x_1, \ldots, x_m) = x_1 a_1 + \cdots + x_m a_m$. Then ϕ is a surjective homomorphism. ■

First Reduction

Let A be a finitely generated abelian group and let $\phi : \mathbb{Z}^m \to A$ be a surjective homomorphism. Let $B = \ker \phi \leq \mathbb{Z}^m$. By the 1^{st} isomorphism theorem, we have $A \cong \mathbb{Z}^m / B$. If:

$$\begin{aligned} B &= d_1\mathbb{Z} \times \cdots \times d_n\mathbb{Z} \times \{0\} \times \cdots \times \{0\} \\ &\leq \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{n} \times \underbrace{\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}}_{r := m-n} = \mathbb{Z}^m \end{aligned}$$

then

$$\begin{aligned} A &\cong \mathbb{Z}^m / B \\ &\cong \frac{\mathbb{Z} \times \cdots \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}}{d_1\mathbb{Z} \times \cdots \times d_n\mathbb{Z} \times \{0\} \times \cdots \times \{0\}} \\ &\cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z} \times \mathbb{Z}/\{0\} \times \mathbb{Z}/\{0\} \\ &\cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z} \\ &= \mathbb{Z}d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z} \times \mathbb{Z}^r \\ &\cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z} \end{aligned}$$

where the third line is a result in the exercise sheet. However, B might not have this form.

Lemma

If $\phi : G_1 \to G_2$ is an isomorphism, $N_1 \trianglelefteq G_1$, $N_2 \trianglelefteq G_2$, and $\phi(N_1) = N_2$, then

$$\begin{aligned} G_1/N_1 &\to G_2/N_2 \\ g_1 N_1 &\mapsto \phi(g_1) N_2 \end{aligned}$$

is a well defined isomorphism.

We can actually make this result more general:

Let $\phi : G_1 \to G_2$ be a homomorphism and $N_2 \trianglelefteq G_2$. Then $\phi^{-1}(N_2) \trianglelefteq G_1$ and the map

$$\begin{aligned} G_1/\phi^{-1}(N_1) &\to G_2/N_2 \\ g_1\phi^{-1}(N_1) &\mapsto \phi(g_1)N_2 \end{aligned}$$

is a well defined injective homomorphism with $\operatorname{im}\phi = \phi(G_1)N_2/N_2$.

To prove that an inversion factor decomposition exists, it suffices to construct an isomorphism $\mathbb{Z}^m \to \mathbb{Z}^m$ that maps B to $d_1\mathbb{Z} \times \cdots \times d_n\mathbb{Z} \times \{0\} \times \cdots \times \{0\}$, where $d_1, \ldots, d_n \in \mathbb{Z}_{>0}$ such that $d_1|\cdots|d_n$. Indeed, if this is the case then from the first reduction section, we would have shown that

$$A \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_n\mathbb{Z} \tag{11}$$

To construct an isomorphism $\mathbb{Z}^m \to \mathbb{Z}^m$ that maps B to the prescribed subgroup of $\mathbb{Z}^m$, we need a better understanding of group isomorphisms to $\mathbb{Z}^m$, especially their subgroups and isomorphisms between them. This leads us to the study of free abelian groups, which we have done in the first section.

Second Reduction

Let A be a finitely generated abelian group, $\phi : \mathbb{Z}^m \to A$ is a surjective homomorphism, and $B = \ker\phi \leq \mathbb{Z}^m$. Recall that it suffices to construct an isomorphism $\mathbb{Z}^m \to \mathbb{Z}^m$ that maps B to

$$d_1\mathbb{Z} \times \cdots \times d_n\mathbb{Z} \times \{0\} \times \cdots \times \{0\} \leq \mathbb{Z}^m$$

for some positive integers $d_1|\cdots|d_n$.

Since $B \leq \mathbb{Z}^m$, we now know that B is a free abelian group of rank $n \leq m$. Let $r = m - n$. It then suffices to prove the following theorem (too lazy to write proof, can be found in Lec 20):

Let C be a free abelian group of finite rank m and let $B \leq C$. Then B is a free abelian group of rank at most m. Let $n = \operatorname{rank}(B) \leq m$.

Then, there exists bases $\beta = \{b_1, \ldots, b_n\}$ of B and $\gamma = \{c_1, \ldots, c_m\}$ of C and positive integers $d_1|\cdots|d_n$ such that

$$b_i = d_i c_i$$

for all $i = 1, \ldots, n$. Moreover, $d_1, \ldots, d_n$ are unique.

Indeed, suppose that this theorem holds and apply it to $B = \ker\phi \leq \mathbb{Z}^n = C$. The isomorphism

$$\mathbb{Z}^m = C \xrightarrow{[\cdot]_\gamma} \mathbb{Z}^m$$

maps $b_i = d_i c_i$ to $d_i e_i$ for all $i = 1, \ldots, n$. Therefore, the isomorphism maps B to $d_1\mathbb{Z} \times \cdots \times d_n\mathbb{Z} \times \{0\} \times \cdots \times \{0\}$.

We will prove a more general theorem.

Let B and C be free abelian groups of finite ranks n and m, respectively. Let $\Psi : B \to C$ be a homomorphism.

Then there exists bases $\beta = \{b_1, \ldots, b_n\}$ of B and $\gamma = \{c_1, \ldots, c_m\}$ of C, there exists a positive integer $r \leq m, n$ and there exists positive integers $d_1|\cdots|d_r$ such that

$$\Psi(b_i) = \begin{cases} d_i c_i & 1 \leq i \leq r \\ 0 & r < i \leq n \end{cases}$$

or equivalently

$$[\Psi]_\gamma^\beta = \left[\begin{array}{ccc|c} d_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & d_r & \\ \hline & 0 & & 0 \end{array}\right]$$

Moreover, $r, d_1, \ldots, d_r$ are unique.

Let β_0, γ_0 be bases of B, C, respectively. The theorem is equivalent to the assertion that there exists matrices $P \in \mathsf{GL}_m(\mathbb{Z})$, $Q \in \mathsf{GL}_n(\mathbb{Z})$ such that

$$P[\Psi]_{\gamma_0}^{\beta_0} Q = \left[\begin{array}{ccc|c} d_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & d_r & \\ \hline & 0 & & 0 \end{array}\right]$$

for some positive integers $d_1 | \cdots | d_r$, and $r, d_1, \ldots, d_r$ are unique. It turns out that slightly more is true.

Uniqueness

Now that we have shown it is possible to create an invariant factor decomposition, let us show this is unique. To do this, we make use of torsion subgruops.

Torsion Subgroup

Definition Torsion subgroup of A
Let A be an abelian group. For each $n \in \mathbb{Z}_{>0}$, we define the n-torsion subgroup of A to be

$$A[n] := \{a \in A : na = 0\}$$

we define the n-power torsion subgroup of A to be

$$A[n^\infty] := \left\{a \in A : n^k a = 0 \text{ for some } k \in \mathbb{Z}_{\geq 0}\right\}$$

and we define the torsion subgroup of A to be

$$\mathsf{Tor}(A) := \{a \in A : ma = 0 \text{ for some } m \in \mathbb{Z}_{>0}\} = \bigcup_{n \in \mathbb{Z}_{>0}} A[n].$$

Proposition 2.1 Isomorphisms of Torsion Groups

Let A be a finitely generated group. If $A \cong \mathbb{Z}^r \times T$, where $r \in \mathbb{Z}_{\geq 0}$ and T is a finite abelian group, then $T \cong \mathsf{Tor}(A)$ and $\mathbb{Z}^r \cong A/\mathsf{Tor}(A)$.

Consequently, T is unique up to isomorphism and r is unique.

Proof: First, note that if $\phi : B \to C$ is an isomorphism between abelian groups, then $\phi(\mathsf{Tor}B) = \mathsf{Tor}C$, so ϕ restricts to an isomorphism $\phi : \mathrm{Tor}B \to \mathrm{Tor}C$.

Let $\phi : A \to \mathbb{Z}^r \times T$ be an isomorphism as in the proposition statement.

Since $\mathrm{Tor}(\mathbb{Z}^r \times T) = \{(0, \ldots, 0)\} \times T \cong T$, we have $\mathrm{Tor}(A) \cong \{0\} \times T \cong T$.

Also since $\phi(\mathrm{Tor}A) = \{0\} \times T$, the map

$$\begin{gathered} A/\mathrm{Tor}A \to \mathbb{Z}^r \times T/(\{0\} \times T) \\ a + \mathrm{Tor}A \mapsto \phi(a) + (\{0\} \times T) \end{gathered}$$

is a well defined isomorphism. Therefore,

$$\begin{aligned} A/\mathrm{Tor} A &\cong \mathbb{Z}^r \times T/(\{0\} \times T) \\ &\cong \mathbb{Z}^r/\{0\} \times T/T \\ &\cong \mathbb{Z}^r \times \{0\} \\ &\cong \mathbb{Z}^r \end{aligned}$$

■

Proposition 2.2: Isomorphisms of n-power Torsion Groups

Let A be a finitely generated abelian group. If $A \cong \mathbb{Z}^r \times P \times B$, where $r \in \mathbb{Z}_{\geq 0}$, P is a finite abelian group with $|P| = p^k$ for some prime p, and B is a finite abelian group with $p \nmid |B|$, then

$$A[p^\infty] \cong P$$

Proposition 2.3: Uniqueness

To prove uniqueness of the invariant factor and elementary divisor decompositions, it remains for us to prove that $d_1, \dots, d_n$ and $e_{i,1}, \dots, e_{i,n_i}$ are unique for each $i = 1, \dots, s$.

Let A be a finite abelian group. If $A \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$ for positive integers $a_1 | \cdots | a_n$, then $a_1, \dots, a_n$ are uniquely determined by A.

To prove this, we make use of the following lemma:

If $a \in \mathbb{Z}$, $b \in \mathbb{Z}_{>0}$, then

$$a(\mathbb{Z}/b\mathbb{Z}) = \gcd(a, b)\mathbb{Z}/b\mathbb{Z}$$

Proof: We have

$$\begin{aligned} a(\mathbb{Z}/b\mathbb{Z}) &= \{a(n + b\mathbb{Z}) : n \in \mathbb{Z}\} \\ &= \{an + b\mathbb{Z} : n \in \mathbb{Z}\} \qquad\qquad = \{x + b\mathbb{Z} : x \in a\mathbb{Z}\} \\ &= \text{ image of } a\mathbb{Z} \text{ under the quotient homomorphism } \mathbb{Z} \to \mathbb{Z}/b\mathbb{Z} \\ &= (a\mathbb{Z} + b\mathbb{Z})/b\mathbb{Z} \\ &= \gcd(a, b)\mathbb{Z}/b\mathbb{Z} \end{aligned}$$

where the last line follows from Bezout's Lemma. ■

and another lemma:

Let p be a prime and let $b \in \mathbb{Z}_{>0}$, for all $e \in \mathbb{Z}_{>0}$, we have

$$\frac{p^{e-1}(\mathbb{Z}/b\mathbb{Z})}{p^e(\mathbb{Z}/b\mathbb{Z})} \cong \begin{cases} \{0\} & p^e \nmid b \\ \mathbb{Z}/p\mathbb{Z} & p^e | b \end{cases}$$

Proof: Let $e \in \mathbb{Z}_{>0}$. By Lemma 1, we have

$$p^{e-1}(\mathbb{Z}/b\mathbb{Z}) = \gcd(p^{e-1}, b)\mathbb{Z}/b\mathbb{Z}$$

and

$$p^e(\mathbb{Z}/b\mathbb{Z}) = \gcd(p^e, b)\mathbb{Z}/b\mathbb{Z}$$

Suppose $p^e \nmid b$. Then $\gcd(p^e, b) = \gcd(p^{e-1}, b)$. Therefore $p^{e-1}(\mathbb{Z}/b\mathbb{Z}) = p^e(\mathbb{Z}/b\mathbb{Z})$, and

$$\frac{p^{e-1}(\mathbb{Z}/b\mathbb{Z})}{p^e(\mathbb{Z}/b\mathbb{Z})} \cong \{0\}$$

Suppose $p^e \mid b$. Then $\gcd(p^e, b) = p^e$ and $\gcd(p^{e-1}, b) = p^{e-1}$. Therefore:

$$\begin{aligned} \frac{p^{e-1}(\mathbb{Z}/b\mathbb{Z})}{p^e(\mathbb{Z}/b\mathbb{Z})} &= \frac{p^{e-1}\mathbb{Z}/b\mathbb{Z}}{p^e\mathbb{Z}/b\mathbb{Z}} \\ &\cong p^{e-1}\mathbb{Z}/p^e\mathbb{Z} \end{aligned}$$

where we have used the third isomorphism theorem. The map

$$\begin{aligned} \mathbb{Z}/p\mathbb{Z} &\to p^{e-1}\mathbb{Z}/p^e\mathbb{Z} \\ n + p\mathbb{Z} &\mapsto p^{e-1}n + p^e\mathbb{Z} \end{aligned}$$

is a well defined isomorphism (consider $\mathbb{Z} \to p^{e-1}\mathbb{Z}/p^e\mathbb{Z}$ and $n \mapsto p^{e-1}n + p^e\mathbb{Z}$ and apply the first isomorphism theorem).

Therefore,

$$p^{e-1}\mathbb{Z}/p^e\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z}$$

and we are done. ■

Let $\phi : A \to \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z} =: B$ be an isomorphism, where $a_1| \cdots |a_n$ are positive integers.

Let p be a prime and $e \in \mathbb{Z}_{>0}$. Then $\phi(p^{e-1}A) = p^{e-1}B$ and $\phi(p^eA) = p^eB$. Therefore, the map

$$\begin{aligned} p^{e-1}A/p^eA &\to p^{e-1}B/p^eB \\ x + p^eA &\mapsto \phi(x) + p^eB \end{aligned}$$

is an isomorphism. We have

$$\begin{aligned} \frac{p^{e-1}A}{p^eA} &\cong \frac{p^{e-1}B}{p^eB} \\ &= \frac{p^{e-1}(\mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z})}{p^e(\mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z})} \\ &= \frac{p^{e-1}(\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times p^{e-1}(\mathbb{Z}/a_n\mathbb{Z})}{p^e(\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times p^e(\mathbb{Z}/a_n\mathbb{Z})} \\ &\cong \frac{p^{e-1}(\mathbb{Z}/a_1\mathbb{Z})}{p^e(\mathbb{Z}/a_1\mathbb{Z})} \times \cdots \times \frac{p^{e-1}(\mathbb{Z}/a_n\mathbb{Z})}{p^e(\mathbb{Z}/a_n\mathbb{Z})} \\ &\cong (\mathbb{Z}/p\mathbb{Z})^r \end{aligned}$$

where r is the number of $i \in \{1, \ldots, n\}$ such that $p^e|a_i$.

Let $i \in \{1, \ldots, n\}$.

If $p^e|a_i$, then $p^e|a_i, a_{i+1}, \ldots, a_n$, so there are at least $n - (i - 1)$ elements $j \in \{1, \ldots, n\}$ such that $p^e|a_j$ and therefore

$$r \geq n - (i - 1).$$

If $p^e \nmid a_i$, then $p^e \nmid a_1, \ldots, a_i$, so $r \leq n - i$.

Therefore $p^e|a_i$ if and only if $p^{e-1}A/p^eA \cong (\mathbb{Z}/p\mathbb{Z})^r$ for some $r \geq n - (i - 1)$ if and only if $|p^{e-1}A/p^eA| = p^r$ for some $r \geq n - (i - 1)$.

Thus the prine powers that divide each a_i are determined by A and therefore the a_i are determined by A.

Elementary Divisors to Inversion Factors

Now we wish to show we can create an isomorphism between the two ways to decompose an abelian group, and thus show that they are equivalent.

Suppose that $A \cong \mathbb{Z}^r \times \prod_{i=1}^{s} \prod_{j=1}^{n_i} \mathbb{Z}/(p_i^{e_{i,j}}\mathbb{Z})$. Recall that $p_1 < \cdots < p_S$ and $e_{i,1} \geq \cdots \geq e_{i,n_i}$ for all $i = 1, \dots, s$.

Let $n = \max_{1 \leq i \leq s}(n_i)$. For each $i \in \{1, \dots, s\}$, if $n_i < n$, define $e_{ij} = 0$ for all $n_i < j \leq n$. Then

$$\begin{aligned} A &\cong \mathbb{Z}^r \times \prod_{i=1}^{s} \prod_{j=1}^{n} \mathbb{Z}/(p_i^{e_{i,j}}\mathbb{Z}) \\ &\cong \mathbb{Z}^r \times \prod_{j=1}^{n} \prod_{i=1}^{s} \mathbb{Z}/(p_i^{e_{i,j}}\mathbb{Z}). \end{aligned}$$

Now,

$$\prod_{i=1}^{s} \mathbb{Z}/(p_i^{e_{i,j}}\mathbb{Z}) \cong \mathbb{Z}/(p_1^{e_{1,j}} \cdots p_n^{e_{n,j}}\mathbb{Z})$$

for all $j = 1, \dots, n$.

Define $d_i = p_1^{e_{1,n-i+1} \cdots p_n^{e_{n,n-i+1}}}$ for $i = 1, \dots, n$. Then $d_1 | \cdots | d_n$ and

$$A \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$$