Abelian groups- the (un)building blocks

Summer Seminar Series
Summer 2025
Theoretical Nexus

Purnima Tiwari

Department of Mathematics

June 2, 2025

purnima162.21@gmail.com

Outline

"I can see the sun, but even if I cannot see the sun, I know that it exists. And to know that the sun is there - that is living."

— Fyodor Dostoevsky, The Brothers Karamazov

Fundamental Theorem of Finitely Generated Abelian Groups- *a breakdown*

Fundamental Theorem of Finitely Generated Abelian Groups- *a breakdown*

Theorem

Let G be a finitely generated abelian group. Then G is isomorphic to a direct sum of cyclic groups:

$$G \cong \mathbb{Z}^n \oplus \mathbb{Z}_{q_1^{k_1}} \oplus \mathbb{Z}_{q_2^{k_2}} \oplus \cdots \oplus \mathbb{Z}_{q_t^{k_t}},$$

where:

- $\mathbb{Z}^n$ *is the* ***free abelian group*** *of rank $n \geq 0$ (the number of infinite components),*
- $\mathbb{Z}_{q_i^{k_i}}$ *are* ***finite cyclic groups*** *of prime-power order $q_i^{k_i}$.*

Uniqueness:

- The rank n is uniquely determined.
- The prime powers $q_i^{k_i}$ (called **elementary divisors**) are uniquely determined up to ordering.

Free Abelian Group

Free Abelian Group

A free abelian group is an abelian group that has a basis.

Free Abelian Group

A free abelian group is an abelian group that has a basis.

That is, there exists a subset (called a **basis**) such that every element of the group can be uniquely expressed as a finite linear combination of the basis elements with integer coefficients.

Free Abelian Group

A free abelian group is an abelian group that has a basis.

That is, there exists a subset (called a **basis**) such that every element of the group can be uniquely expressed as a finite linear combination of the basis elements with integer coefficients.

The rank of a free abelian group is the cardinality of a basis.

Free Abelian Group

A free abelian group is an abelian group that has a basis.

That is, there exists a subset (called a **basis**) such that every element of the group can be uniquely expressed as a finite linear combination of the basis elements with integer coefficients.

The rank of a free abelian group is the cardinality of a basis.

The intuitive idea to grasp the concept of rank can be developed from considering it as the number of independent directions that a particle (or an elemnt of a group) is allowed to move in,

Free Abelian Group

A free abelian group is an abelian group that has a basis.

That is, there exists a subset (called a **basis**) such that every element of the group can be uniquely expressed as a finite linear combination of the basis elements with integer coefficients.

The rank of a free abelian group is the cardinality of a basis.

The intuitive idea to grasp the concept of rank can be developed from considering it as the number of independent directions that a particle (or an elemnt of a group) is allowed to move in, which in the case of a free group are infinite, since a free group is, essentially **free**.

Free Group

Free Group

Let S be a set. The **free group** $F(S)$ on S consists of all *reduced words* in $S \cup S^{-1}$ (formal symbols and their inverses), where a word is reduced if no element is adjacent to its inverse.

Free Group

Let S be a set. The **free group** $F(S)$ on S consists of all *reduced words* in $S \cup S^{-1}$ (formal symbols and their inverses), where a word is reduced if no element is adjacent to its inverse.

Multiplication is concatenation followed by reduction. It satisfies the universal property:

Any function

$$f : S \to G$$

G being a group, extends uniquely to a homomorphism

$$\tilde{f} : F(S) \to G$$

Universal Property in Action

Key Insight

The free group $F(S)$ is the **most general** group generated by S such that any map

$$f : S \to G$$

extends uniquely to a homomorphism

$$\phi : F(S) \to G$$

Freedom to map, without relations getting in the way.

Example: Define $\phi : F(a, b) \to S_3$ by:

$$
\begin{aligned}
f(a) &= (1\ 2), \quad f(b) = (1\ 2\ 3) \quad \text{(arbitrary choices)} \\
\phi(ab) &= f(a)f(b) = (1\ 2)(1\ 2\ 3) = (2\ 3), \\
\phi(ba) &= f(b)f(a) = (1\ 2\ 3)(1\ 2) = (1\ 3), \\
\phi(a^2) &= e, \quad \phi(b^{-1}ab) = (1\ 3), \quad \text{and so on} \ldots
\end{aligned}
$$

Step-by-Step Computation

Why this works:

1. **Generators**: $F(a, b)$ has no relations; words like ab and ba are distinct.
2. **Extension**: ϕ substitutes generators and simplifies in S_3:

$$\phi(aba^{-1}b^{-1}) = (1\ 2)(1\ 2\ 3)(1\ 2)(1\ 3\ 2) = (1\ 3\ 2).$$

3. **Verification**: Check $\phi(w_1 w_2) = \phi(w_1)\phi(w_2)$:

$$\phi(b^{-1}ab) = \phi(b^{-1})\phi(ab) = (1\ 3\ 2)(2\ 3) = (1\ 3).$$

Free Abelian Group

Free Abelian Group

Definition: Abelian group with basis $B \subset G$

1. B generates G
2. Linear independence:

$$\sum n_i b_i = 0 \Rightarrow n_i = 0$$

- Isomorphic to $\mathbb{Z}^n$ for finite rank n.

3. and **uniqueness**!

Example: $\mathbb{Z}^2$ with basis $\{(1,0),(0,1)\}$
Non-example: $\mathbb{Z}/n\mathbb{Z}$ (torsion)

The word *torsion* comes from the Latin *torquere* (<u>to twist</u>), like twisting a rope until it loops back.

Direct vs. Internal Sums/Products

Key Definitions

Let G be a group and H, K be subgroups.

1. Direct Product (External):

$$G = H \times K := \{(h, k) \mid h \in H, k \in K\}, \quad \text{with component-wise operation.}$$

2. Direct Sum (External): For *abelian* groups, $H \oplus K$ is the same as $H \times K$.

3. Internal Direct Product: G is the *internal* direct product of H and K if:

- $G = HK$ (every $g \in G$ is $g = hk$),
- $H \cap K = \{e\}$,
- H, K are normal in G.

4. Internal Direct Sum: For *abelian* groups, replace "normal" with "subgroups" and write $G = H \oplus K$.

Key Insight

External constructs new groups from old.
Internal decomposes existing groups into simpler pieces.

The Fundamental Theorem

The Fundamental Theorem

Theorem

Every finitely generated abelian group G decomposes as:

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$$

where:

- $r \geq 0$ *(free rank)*
- $d_i > 1$ *with* $d_{k-1} \mid d_k$

Example

$G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$

Example

$G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$

Primary decomposition:
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

Example

$G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$

Primary decomposition:
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

Invariant factors:
$d_1 = 2^1 \cdot 3^1 \cdot 5^0 = 6$
$d_2 = 2^1 \cdot 3^1 \cdot 5^1 = 30$
Since $6 \mid 30$, $G \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$

Key Definitions

Torsion Subgroup

For an abelian group G:

$$T(G) = \{g \in G \mid \exists\ 0 < n < \infty : g^n = e\}$$

Example: $G = \mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ then $T(G) = \{e\} \times \mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/6\mathbb{Z}$

Key Definitions

Torsion Subgroup

For an abelian group G:

$$T(G) = \{g \in G \mid \exists\, 0 < n < \infty : g^n = e\}$$

Example: $G = \mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ then $T(G) = \{e\} \times \mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/6\mathbb{Z}$

A torsion subgroup, in the simplest terms, consists of all the elements of the group which have a finite order.

Torsion-Free Group

G is torsion-free if $T(G) = \{e\}$

Example: $\mathbb{Z}^n$, $\mathbb{Q}$

Non-example: $\mathbb{Z}/n\mathbb{Z}$

The Proof.

We elaborate the steps henceforth and will develop an intuition for the proof, whilst also determining the special case.

Theorem

If G is finitely generated abelian, then:

1. $T(G)$ *is a finite subgroup*
2. $G/T(G)$ *is torsion-free and finitely generated*
3. $G/T(G)$ *is free abelian* $\cong \mathbb{Z}^r$

Example: $G = \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$T(G) = \{0\} \times \mathbb{Z}/2\mathbb{Z}$, $G/T(G) \cong \mathbb{Z}$

p-primary Component

For prime p:

$$T_p(G) = \{g \in T(G) \mid g^{p^k} = 0 \text{ for some } k\}$$

Theorem (Primary Decomposition)

$$T(G) \cong \bigoplus_{p \text{ prime}} T_p(G)$$

Example: $T(G) = \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
$T_2(G) \cong \mathbb{Z}/2\mathbb{Z}$, $T_3(G) \cong \mathbb{Z}/3\mathbb{Z}$

The Fundamental Theorem for Finite Abelain Groups

The Fundamental Theorem for Finite Abelian Groups

Theorem

A finite abelian p-group decomposes as:

$$H \cong \mathbb{Z}/p^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{e_k}\mathbb{Z}, \quad e_1 \leq e_2 \leq \cdots \leq e_k$$

Example

$T(G) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$

1. Primary decomposition:

$$T_2(G) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/2^1\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z}$$
$$T_3(G) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \cong \mathbb{Z}/3^1\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z}$$

2. Exponents by prime:

	Component 1	Component 2
p=2	1	2
p=3	1	2

3. Form invariant factors:

$$d_1 = 2^{\min(1,2)} \times 3^{\min(1,2)} = 2^1 \times 3^1 = 6$$
$$d_2 = 2^{\max(1,2)} \times 3^{\max(1,2)} = 2^2 \times 3^2 = 36$$

4. $6|36$ so $T(G) \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$

dissecting the theorem:

dissecting the theorem:

$$G \cong \underbrace{\mathbb{Z}^r}_{\text{free part}} \times \underbrace{\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}}_{\text{torsion part}}$$

with $d_1 \mid d_2 \mid \cdots \mid d_k > 1$

dissecting the theorem:

$$G \cong \underbrace{\mathbb{Z}^r}_{\text{free part}} \times \underbrace{\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}}_{\text{torsion part}}$$

with $d_1 \mid d_2 \mid \cdots \mid d_k > 1$

Uniqueness:

- $r = \dim_{\mathbb{Q}}(G \otimes \mathbb{Q})$ (free rank)
- $d_k = \exp(T(G))$ (exponent of torsion subgroup)
- $d_{k-1}d_k = \exp(T(G)/\langle\text{elem of order } d_k\rangle)$ etc.

Example: $G = \mathbb{Z}^2 \times \mathbb{Z}/4\mathbb{Z}$
$r = 2,\ T(G) = \mathbb{Z}/4\mathbb{Z} \Rightarrow d_1 = 4$
Decomposition: $\mathbb{Z}^2 \times \mathbb{Z}/4\mathbb{Z}$

What if the free part has rank zero?

What if the free part has rank zero?

The theorem then is referred to as the Fundamental Theorem of Finite abelian Groups!

Fundamental Theorem of Finite Abelian Groups (FTFAG)

Theorem Statement

Every finite abelian group G is isomorphic to a direct sum of cyclic groups of prime-power order:

$$G \cong \mathbb{Z}_{p_1^{k_1}} \oplus \mathbb{Z}_{p_2^{k_2}} \oplus \cdots \oplus \mathbb{Z}_{p_m^{k_m}},$$

where:

- p_i are primes (not necessarily distinct),
- k_i are positive integers.

Uniqueness

The decomposition is unique up to:

- The order of the factors,
- Rearrangement of the prime powers $p_i^{k_i}$.

Example

The group $\mathbb{Z}/6\mathbb{Z}$ decomposes as:

$$\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3.$$

Thank you.