Fundamental Theorem of Finitely Generated Abelian Groups

Kevin James

Definition

1. A group G is finitely generated if there is a finite subset $A \subseteq G$ such that $G = < A >$.
2. For each $0 \leq r \in \mathbb{Z}$, let $\mathbb{Z}^r = \mathbb{Z} \times \cdots \times \mathbb{Z}$ be the direct product of r copies of $\mathbb{Z}$, where we take $\mathbb{Z}^0 = 1$. The group $\mathbb{Z}^r$ is a free abelian group of rank r.

Definition

1. A group G is finitely generated if there is a finite subset $A \subseteq G$ such that $G = < A >$.
2. For each $0 \leq r \in \mathbb{Z}$, let $\mathbb{Z}^r = \mathbb{Z} \times \cdots \times \mathbb{Z}$ be the direct product of r copies of $\mathbb{Z}$, where we take $\mathbb{Z}^0 = 1$. The group $\mathbb{Z}^r$ is a free abelian group of rank r.

Theorem (Fundamental Theorem of Finitely Generated Abelian Groups)

Let G be a finitely generated Abelian group. Then,

1. $G \cong \mathbb{Z}^r \times Z_{n_1} \times \cdots \times Z_{n_s}$ *for some integers* $r, n_1, \ldots, n_s$ *satisfying the following conditions.*
   1. $r \geq 0$ *and* $n_j \geq 2$ *for* $1 \leq j \leq s$, *and*
   2. $n_{i+1} | n_i$ *for* $1 \leq i \leq (s-1)$.
2. *The expression above is unique.*

Definition

The integer r in the above Theorem is called the free rank or Betti number of G and the integers n_i are called the invariant factors of G. The description of G in the Theorem is called the invariant factor decomposition of G.

Note

1. Two finitely generated Abelian groups are isomorphic if and only if they have the same free rank and the same invariant factors.
2. All finite Abelian groups are finitely generated.
3. A finitely generated Abelian group is finite if and only if its free rank is 0.
4. The finite Abelian groups are given up to isomorphism by the various $Z_{n_1} \times \cdots \times Z_{n_s}$ where
    1. $n_j \geq 2$,
    2. $n_{i+1} | n_i$,
    3. $n_1 \cdot n_2 \cdot \cdots \cdot n_s = n$.
    4. Every prime divisor of n must divide n_1.

Corollary

If n is the product of distinct primes and G is an Abelian group of order n, then $G \cong Z_n$.

Corollary

If n is the product of distinct primes and G is an Abelian group of order n, then $G \cong Z_n$.

Theorem

Let G be an abelian group of order $n > 1$ and let the unique factorization of n into distinct prime powers be given by $n = p_1^{a_1} \dots p_k^{a_k}$. Then,

1. *$G \cong A_1 \times \cdots \times A_k$, where $|A_i| = p_i^{a_i}$*
2. *for each $A \in \{A_1, \dots, A_k\}$ with $|A| = p^a$,*

$$A \cong Z_{p^{b_1}} \times \cdots \times Z_{p^{b_t}}$$

   with $b_1 \geq b_2 \geq \cdots \geq b_t$ and $b_1 + \cdots + b_t = a$

3. *The decomposition given above is unique.*

DEFINITION

The integers p^{b_i} described in the preceding theorem are called the elementary divisors of G. The description of G in the first parts of the theorem is called the elementary divisor decomposition of G.

Definition

The integers p^{b_i} described in the preceding theorem are called the elementary divisors of G. The description of G in the first parts of the theorem is called the elementary divisor decomposition of G.

Note

1. The A_i are the Sylow p-subgroups of G. Thus a finite Abelian group is the direct product of its Sylow p-subgroups.
2. The decomposition of A_i appearing in the 2nd part of the theorem is the invariant factor decomposition of A_i. So the elementary divisors of G are the invariant factors of the Sylow p-subgroups as p varies over all primes dividing $|G|$.

Proposition

Let $0 < m, n \in \mathbb{Z}$*.*

1. $Z_m \times Z_n \cong Z_{mn}$ *if and only if* $(m, n) = 1$*.*
2. *If* $n = p_1^{a_1} \dots p_k^{a_k}$*, then* $Z_n \cong Z_{p_1^{a_1}} \times \cdots \times Z_{p_k^{a_k}}$*.*

Proposition

Let $0 < m, n \in \mathbb{Z}$.

1. $Z_m \times Z_n \cong Z_{mn}$ *if and only if* $(m, n) = 1$.
2. *If* $n = p_1^{a_1} \dots p_k^{a_k}$, *then* $Z_n \cong Z_{p_1^{a_1}} \times \cdots \times Z_{p_k^{a_k}}$.

Definition

1. If G is a finite abelian group of type $(n_1, \dots, n_t)$, the integer t is called the rank of G.
2. If G is any group, the exponent of G is the smallest positive integer n such that $x^n = 1, \forall x \in G$. If no such n exists we say that the exponent is ∞.