The Fundamental Theorem of Finite Abelian Groups!

Every finite Abelian group is isomorphic to a unique group of the form

$$\mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$$

where the numbers p_i are not necessarily distinct primes, up to a reordering of the terms in the product.

The Fundamental Theorem of Finite Abelian Groups!

Every finite Abelian group is isomorphic to a unique group of the form

$$\mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$$

where the numbers p_i are not necessarily distinct primes, up to a reordering of the terms in the product.

Cool Facts about the Fundamental Theorem:

- Allows us to classify all finite Abelian groups!

The Fundamental Theorem of Finite Abelian Groups!

Every finite Abelian group is isomorphic to a unique group of the form

$$\mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$$

where the numbers p_i are not necessarily distinct primes, up to a reordering of the terms in the product.

Cool Facts about the Fundamental Theorem:

- Allows us to classify all finite Abelian groups!
- The numbers $p_i^{n_i}$ are called the *elementary divisors* of G. We can also write G uniquely as $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_j}$ where $m_1 | m_2 | \cdots | m_j$. The numbers m_i are called *invariant factors* of G.

The Fundamental Theorem of Finite Abelian Groups!

Every finite Abelian group is isomorphic to a unique group of the form

$$\mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$$

where the numbers p_i are not necessarily distinct primes, up to a reordering of the terms in the product.

Cool Facts about the Fundamental Theorem:

- Allows us to classify all finite Abelian groups!
- The numbers $p_i^{n_i}$ are called the *elementary divisors* of G. We can also write G uniquely as $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_j}$ where $m_1 | m_2 | \cdots | m_j$. The numbers m_i are called *invariant factors* of G.
- The theorem can be generalized to the Fundamental Theorem of Finitely Generated Abelian Groups, including some copies of $\mathbb{Z}$.

The Fundamental Theorem of Finite Abelian Groups!

Every finite Abelian group is isomorphic to a unique group of the form

$$\mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$$

where the numbers p_i are not necessarily distinct primes, up to a reordering of the terms in the product.

Cool Facts about the Fundamental Theorem:

- Allows us to classify all finite Abelian groups!
- The numbers $p_i^{n_i}$ are called the *elementary divisors* of G. We can also write G uniquely as $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_j}$ where $m_1|m_2|\cdots|m_j$. The numbers m_i are called *invariant factors* of G.
- The theorem can be generalized to the Fundamental Theorem of Finitely Generated Abelian Groups, including some copies of $\mathbb{Z}$.
- There's an algorithm to find this decomposition for a given G!

The Fundamental Theorem of Finite Abelian Groups!

Every finite Abelian group is isomorphic to a unique group of the form

$$\mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$$

where the numbers p_i are not necessarily distinct primes, up to a reordering of the terms in the product.

Cool Facts about the Fundamental Theorem:

- Allows us to classify all finite Abelian groups!
- The numbers $p_i^{n_i}$ are called the *elementary divisors* of G. We can also write G uniquely as $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_j}$ where $m_1 | m_2 | \cdots | m_j$. The numbers m_i are called *invariant factors* of G.
- The theorem can be generalized to the Fundamental Theorem of Finitely Generated Abelian Groups, including some copies of $\mathbb{Z}$.
- There's an algorithm to find this decomposition for a given G!
- The converse of Lagrange's Theorem is true for Abelian groups.

The Fundamental Theorem of Finite Abelian Groups!

Every finite Abelian group is isomorphic to a unique group of the form

$$\mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$$

where the numbers p_i are not necessarily distinct primes, up to a reordering of the terms in the product.

Cool Facts about the Fundamental Theorem:

- Allows us to classify all finite Abelian groups!
- The numbers $p_i^{n_i}$ are called the *elementary divisors* of G. We can also write G uniquely as $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_j}$ where $m_1 | m_2 | \cdots | m_j$. The numbers m_i are called *invariant factors* of G.
- The theorem can be generalized to the Fundamental Theorem of Finitely Generated Abelian Groups, including some copies of $\mathbb{Z}$.
- There's an algorithm to find this decomposition for a given G!
- The converse of Lagrange's Theorem is true for Abelian groups.
- Hard to prove but much easier than the corresponding Classification of Finite Simple Groups.

Every finite Abelian group G is isomorphic to a unique group of the form $\mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$

Proof.

1. **$G = H_1 \times H_2 \times \cdots \times H_k$ where $|H_i| = p_i^{n_i}$ for p_i prime.**
   (H_i not necessarily cyclic.)
   Let $|G| = p^n m$ where $p \not| m$, and let $H = \{x \in G \mid x^{p^n} = e\}$ and $K = \{x \in G \mid x^m = e\}$.
   - **a.** $H \leq G$ and $K \leq G$.
   - **b.** $HK = G$. (by Bézout's Identity)
   - **c.** $H \cap K = \{e\}$.
   - **d.** $G = H \times K$.
   - **e.** $|H||K| = p^n m$.
   - **f.** $p \not| |K|$.
   - **g.** $|H| = p^n$.
   - **h.** $G = H_1 \times H_2 \times \cdots \times H_k$ where $|H_i| = p_i^{n_i}$ for p_i prime. (Induction)

Every finite Abelian group G is isomorphic to a unique group of the form $\mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$

2. $H_i = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_t \rangle$ **for elements** $a_1, a_2, \ldots, a_t \in H_i$**.**

- **a.** Let $a \in H_i$ with maximal order $|a| = p^m$. If $m = n_i$ then $H_i = \langle a \rangle$.
- **b.** $x^{p^m} = e$ for all $x \in H_i$.
- **c.** Let $b \notin \langle a \rangle$ with minimal order. $|b^p| = |b|/p$.
- **d.** $b^p = a^j$ for some integer j.
- **e.** $|b^p| \leq p^{m-1}$.
- **f.** $p|j$, so $pr = j$ for some integer r.
- **g.** Let $c = a^{-r}b$. $c \notin \langle a \rangle$.
- **h.** $|c| = p$.
- **i.** $|b| = p$.
- **j.** $\langle a \rangle \cap \langle b \rangle = \varnothing$.
- **k.** Let $\overline{H} = H_i/\langle b \rangle$. In $\overline{H}$, $|\overline{a\langle b \rangle}| = p^m$.
- **l.** $\overline{H} = \langle a\langle b \rangle \rangle \times \overline{L}$ for some $\overline{L} \leq \overline{H}$. (Induction hypothesis)
- **m.** Let $\phi : H_i \to \overline{H}$ be given by $\phi(x) = x\langle b \rangle$, and $L = \phi^{-1}(\overline{L})$. $\langle a \rangle \cap L = \varnothing$.
- **n.** $H_i = \langle a \rangle L$.
- **o.** $H_i = \langle a \rangle \times L$.
- **p.** $H_i = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_t \rangle$ for elements $a_1, a_2, \ldots, a_t \in H_i$. (Induction)

Every finite Abelian group G is isomorphic to a unique group of the form $\mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$

3. **If $H_i = C_1 \times C_2 \times \cdots \times C_k$ for cyclic groups with $|C_1| \geq |C_2| \geq \ldots \geq |C_k|$ and $H_i = D_1 \times D_2 \times \cdots \times D_j$ for cyclic groups with $|D_1| \geq |D_2| \geq \ldots \geq |D_j|$ then $k = j$ and $C_1 \approx D_1$, $C_2 \approx D_2$, ..., $C_k \approx D_k$.**
   a. If $k = 1$ and $j = 1$ then $C_1 \approx C_2$.
   b. $H_i^p = \{h^p \mid h \in H_i\}$ is a proper subgroup of H_i.
   c. $H_i^p = C_1^p \times C_2^p \times \cdots \times C_{k'}^p$ where k' is the largest value of i for which $|C_i| > p$ and $H_i^p = D_1^p \times D_2^p \times \cdots \times D_{j'}^p$ where j' is the largest value of i for which $|D_i| > p$.
   d. $k' = j'$ and $C_1^p \approx D_1^p$, $C_2^p \approx D_2^p$, ..., $C_{k'}^p \approx D_{j'}^p$. (Induction hypothesis)
   e. $k - k' = j - j'$.
   f. $k = j$ and $C_1 \approx D_1$, $C_2 \approx D_2$, ..., $C_k \approx D_k$.
4. **G is isomorphic to a unique group of the form $\mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$.**
   a. G is isomorphic to such a group.
   b. This group is unique.

□