Fundamental Theorem of Finite Abelian Groups

Monica Agana

Boise State University

September 1, 2015
Every finite Abelian group is a direct product of cyclic groups of prime-power order. The number of terms in the product and the orders of the cyclic groups are uniquely determined by the group.
In other words, every finite Abelian group $G$ is isomorphic to a group with the form

$$Z_{p_1^{n_1}} \oplus Z_{p_2^{n_2}} \oplus \cdots \oplus Z_{p_k^{n_k}},$$

such that the $p_i's$ do not have to be distinct primes and the prime-powers $p_1^{n_1}, p_2^{n_2}, \cdots, p_k^{n_k}$ are uniquely determined by $G$. 
“Because of the length and complexity of the proof” to the theorem, it suffices to break the proof up into four lemmas.¹
Proof of the Fundamental Theorem

Lemma (1)

Let $G$ be a finite Abelian group of order $p^n m$, where $p$ is a prime that does not divide $m$. Then $G = H \times K$, where $H = \{ x \in G \mid x^{p^n} = e \}$ and $K = \{ x \in G \mid x^m = e \}$. Also, $|H| = p^n$. 
Proof of the Fundamental Theorem

Lemma (2)

Let $G$ be an Abelian group of prime-power order and let $a$ be an element of maximal order in $G$. Then $G$ can be written in the form $\langle a \rangle \times K$. 
Proof of the Fundamental Theorem

Lemma (3)

A finite Abelian group of prime-power order is an internal direct product of cyclic groups.
Proof of the Fundamental Theorem

*Sketch of Proof (Lemma 3):*

Let $G$ be a finite Abelian group of prime-power order. We want to show $G$ is an internal direct product of cyclic groups.

Recall,

**Definition (pg. 188)**

We say $G$ is the *internal direct product* of $H$ and $K$ and write $G = H \times K$ if $H$ and $K$ are normal subgroups of $G$ and,

1. $G = HK$ and
2. $H \cap K = \{e\}$ (identity)

where the set $HK = \{hk \mid h \in H, k \in K\}$. 
The proof proceeds by induction on $n$. It is easy to see that

**Base Case:** When $n = 1$, $|G| = p^1 = p$. So $G \cong Z_p$.

Next, pick some $x$ of $G$ of maximal possible order, and let $H$ be the subgroup such that $H = \langle x \rangle$. 
Proof of the Fundamental Theorem

The idea is to show that there exists a subgroup $K$ of $G$ where $G$ is the internal direct product of cyclic subgroups.

One can verify that induction on $n$ works by referring to a detailed proof in:

Lemma (4)

Suppose that $G$ is a finite Abelian group of prime-power order. If $G = H_1 \times H_2 \times \cdots \times H_m$ and $G = K_1 \times K_2 \times \cdots \times K_n$, where the $H$’s and $K$’s are nontrivial cyclic subgroups with $|H_1| \geq |H_2| \geq \cdots \geq |H_m|$ and $|K_1| \geq |K_2| \geq \cdots \geq |K_m|$ then $m = n$ and $|H_i| = |K_i|$ for all $i$. 

$\blacksquare$
Purpose of Lemma’s 1-4 in terms of the Fundamental Theorem

**Lemma 1** shows that $G = G(p_1) \times G(p_2) \times \cdots \times G(p_n)$ where each of the $G(p_i)$’s is a group of prime power order.

**Lemma 2** is used to prove Lemma 3.

**Lemma 3** shows that each of these factors is an internal direct product of cyclic groups.

**Lemma 4** proves the uniqueness portion of the Fundamental Theorem.
The Fundamental Theorem allows us an algorithm for “constructing all Abelian groups” of any order that we want.
For example, consider groups whose orders have the form $p^k$ where $p$ is prime and $k \leq 4$.

If $k$ can be written as
\[
k = n_1 + n_2 + \cdots + n_t,
\]
where each $n_i \ (i = 1, 2, \ldots, t)$ is a positive integer, then
\[
\mathbb{Z}_{p^{n_1}} \oplus \mathbb{Z}_{p^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_t}}
\]
is an Abelian group with order $p^k$. 
Again, considering groups of order $p^k$ for $k \leq 4$, we will look at the

1. order of $G$,
2. partitions of $k$, and
3. possible direct products for $G$. 
Fundamental Theorem of Finite Abelian Groups

When $|G| = p$:

The partition of $k$ is 1.

The possible direct products for $G$ is $Z_p$. 
Fundamental Theorem of Finite Abelian Groups

When $|G| = p^2$:

The partitions of $k$ are 2 and $1 + 1$.

The possible direct products for $G$ is $Z_{p^2}$ and $Z_p \oplus Z_p$, respectively.
Fundamental Theorem of Finite Abelian Groups

When $|G| = p^3$:

The partitions of $k$ are $3$, $2 + 1$, and $1 + 1 + 1$.

The possible direct products of $G$ are:

\[
\begin{align*}
Z_{p^3} \\
Z_{p^2} \oplus Z_{p^1} \\
Z_{p^1} \oplus Z_{p^1} \oplus Z_{p^1}
\end{align*}
\]
Fundamental Theorem of Finite Abelian Groups

When $|G| = p^4$:

The partitions of $k$ are $4$, $3 + 1$, $2 + 2$, $2 + 1 + 1$, $1 + 1 + 1 + 1$.

The possible direct products of $G$ are:

- $Z_{p^4}$,
- $Z_{p^3} \oplus Z_{p^1}$
- $Z_{p^2} \oplus Z_{p^2}$
- $Z_{p^2} \oplus Z_{p^1} \oplus Z_{p^1}$
- $Z_{p^1} \oplus Z_{p^1} \oplus Z_{p^1} \oplus Z_{p^1}$
Fundamental Theorem of Finite Abelian Groups

Note that uniqueness (as in the theorem) “guarantees” that each distinct partition of $k$ “yields distinct isomorphism classes.”
These direct products can be compared using the following cancellation property:

*If $A$ is finite, then*

$$A \oplus B \approx A \oplus C \quad \text{if and only if} \quad B \approx C.$$
Fundamental Theorem of Finite Abelian Groups

For example, consider $Z_4 \oplus Z_4$.

This is not isomorphic to $Z_4 \oplus Z_2 \oplus Z_2$ since $Z_4$ is not isomorphic to $Z_2 \oplus Z_2$.

Verifying this, notice that $Z_2 \oplus Z_2$ does not have an element of order 4:

\[
| (0, 0) | = 1 \\
| (0, 1) | = | (1, 0) | = | (1, 1) | = 2,
\]

but $Z_4$ does have an element of order 4 (i.e. $| 1 | = 4$).
Fundamental Theorem of Finite Abelian Groups

Now let us consider when we construct all Abelian groups of a particular order $n$:

To do this, \textbf{first} we would write $n$ as a prime-power decomposition,

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}.$$
Second, we individually form all Abelian groups of order $p_1^{n_1}$, then $p_2^{n_2}$, etc.
Third, we form all possible external direct products of these groups.

For example, suppose the order $n = 1176$.

Writing 1176 as a prime-power decomposition we have

$$1176 = 2^3 \cdot 3 \cdot 7^2.$$
Fundamental Theorem of Finite Abelian Groups

One can verify all the Abelian groups for each of $2^3$, 3 and $7^2$.

Then we get all the possible external direct products of these groups (in other words, the list of the distinct isomorphism classes of Abelian groups with order 1176):

- $\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49}$
- $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49}$
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49}$
- $\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$
- $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$
Fundamental Theorem of Finite Abelian Groups

There is a shortcut! For the *Greedy Algorithm for an Abelian Group of Order* $p^n$, refer to pg. 221 in Gallian [1].
By consequence of the Fundamental Theorem, we get the following corollary:

**Corollary (Existence of Subgroups of Abelian Groups)**

*If m divides the order of a finite Abelian group G, then G has a subgroup of order m.*

On pg. 155: Example 5, the converse of Lagrange’s Theorem is false. However, this corollary actually proves that the converse of Lagrange’s Theorem holds for finite Abelian groups.
Existence of Subgroups of Abelian Groups

Example

Let $G$ be an Abelian group of order $72 = 2^3 \cdot 3^2$, and suppose we want to create a subgroup of order 12. By the Fundamental Theorem of Finite Abelian Groups, we know $G$ is isomorphic to one of the following:

$$
\begin{align*}
&\mathbb{Z}_8 \oplus \mathbb{Z}_9 \\
&\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \\
&\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \\
&\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \\
&\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \\
&\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3
\end{align*}
$$

we already know that $\mathbb{Z}_8 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_{72}$ has a subgroup of order 12. Suppose that we want to produce a subgroup of order 12 in $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$. We can do this by piecing together all of $\mathbb{Z}_4$ and the subgroup of order 3 in $\mathbb{Z}_9$. In other words, we get $\{(a, 0, b) \mid a \in \mathbb{Z}_4, b \in \{0, 3, 6\}\}$. 