The Fundamental Theorem of Finite Abelian Groups

First, we’ll start with a review of another fundamental theorem:

**Theorem** (Fundamental Theorem of Arithmetic)
If \( x \) is an integer greater than 1, then \( x \) can be written as a product of prime numbers. Moreover, the prime factorization of \( x \) is unique, up to commutativity.

We could state this a bit differently: Every integer \( x \) can be written as a product of powers of distinct primes:
\[
x = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}
\]

**Example** We can write the prime factorization of 360 as
\[
360 = 2^3 \cdot 3^2 \cdot 5^1
\]
and no other integer shares this factorization.

Now, the following theorem may seem more familiar:

**Theorem 1** (The Fundamental Theorem of Finite Abelian Groups)
Every finite Abelian group \( G \) can be written as a direct product of cyclic groups of prime power order:
\[
G \approx \mathbb{Z}_{p_1^{r_1}} \oplus \mathbb{Z}_{p_2^{r_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{r_k}}
\]
where the \( p_i \)'s are not necessarily distinct. In addition, the number of terms in the product, and the order of the cyclic group factors, are uniquely determined by the group.

Before we proceed, note that there is a major difference between the theorems. The factorization of an integer into primes, 
\[
x = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k},
\]
assumes that the primes are distinct. We see no difference between the expressions
\[
12 = 4 \cdot 3 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3
\]
However, since \( \mathbb{Z}_4 \) is not isomorphic to \( \mathbb{Z}_2 \oplus \mathbb{Z}_2 \), then
\[
\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \not\approx \mathbb{Z}_4 \oplus \mathbb{Z}_3
\]
So, a finite Abelian group could be isomorphic to \( \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \), but not to \( \mathbb{Z}_4 \oplus \mathbb{Z}_3 \). The way that we arrange the factors \( \mathbb{Z}_{p_i^{r_i}} \) is therefore unique to the group, and cannot be “simplified” as in the prime factorization of integers.

**Example** We’ll find all possible finite Abelian groups of order 360. We already have the prime factorization
\[
360 = 2^3 \cdot 3^2 \cdot 5^1
\]
We can write this factorization in several ways, arranging powers of like primes together. Each arrangement corresponds to a new Abelian group of order 108:

<table>
<thead>
<tr>
<th>Factorization of 360</th>
<th>Corresponding Abelian Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 )</td>
<td>( \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 )</td>
</tr>
<tr>
<td>( 2 \cdot 4 \cdot 3 \cdot 5 )</td>
<td>( \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 )</td>
</tr>
<tr>
<td>( 8 \cdot 3 \cdot 5 )</td>
<td>( \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 )</td>
</tr>
<tr>
<td>( 2 \cdot 2 \cdot 2 \cdot 9 \cdot 5 )</td>
<td>( \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 )</td>
</tr>
<tr>
<td>( 2 \cdot 4 \cdot 9 \cdot 5 )</td>
<td>( \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 )</td>
</tr>
<tr>
<td>( 8 \cdot 9 \cdot 5 )</td>
<td>( \mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}<em>5 \approx \mathbb{Z}</em>{360} )</td>
</tr>
</tbody>
</table>

If we have a specific Abelian group \( G \) with order 360, we can not identify which of these groups it is isomorphic to without some additional work, which usually involves checking the number of elements in each group with a particular order. But we do know that it’s definitely one of the groups on our list.
Before the next Corollary of the Fundamental Theorem of Finite Abelian Groups, we'll recall:

**Theorem** (Lagrange's Theorem)
If $H$ is a subgroup of a finite group $G$, then the order of $H$ divides the order of $G$.

We also want to remember that the converse of this theorem is false, in general. That is, just because $k$ divides the order of a group $G$, we can't assume $G$ has a subgroup of order $k$. However, the converse is true in a particular case:

**Corollary**
If $G$ is a finite Abelian group and $k$ divides $|G|$, then $G$ has a subgroup of order $k$.

**Example** Suppose $G$ is an Abelian group with order 90. Since 90 is divisible by 6, then $G$ must have a subgroup of order 6.

By the Fundamental Theorem of Finite Abelian Groups, $G$ must be one of the groups on the following list:

<table>
<thead>
<tr>
<th>Factorization of 90</th>
<th>Corresponding Abelian Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2 \cdot 3 \cdot 3 \cdot 5$</td>
<td>$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$</td>
</tr>
<tr>
<td>$2 \cdot 9 \cdot 5$</td>
<td>$\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$</td>
</tr>
</tbody>
</table>

If $G \approx \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$, then by Theorem ??,

$$G \approx \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_6 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{15} \approx \mathbb{Z}_6 \oplus \mathbb{Z}_{15}$$

It's easiest to see that the last “version” of our group, $\mathbb{Z}_6 \oplus \mathbb{Z}_{15}$, does have a subgroup $H$ of order 6:

$$H = \{(a, 0) : a \in \mathbb{Z}_6\} = \{(0, 0), (1, 0), (2, 0), (3, 0), (4, 0), (5, 0)\}$$

On the other hand, if $G \approx \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$, then we can form a subgroup $H$ of order 6 by taking the product of $\mathbb{Z}_2$, a subgroup of order 3 from $\mathbb{Z}_9$ (specifically, the subgroup $\langle 3 \rangle = \{0, 3, 6\}$, and the identity from $\mathbb{Z}_5$:

$$H = \{(a, b, 0) : a \in \{0, 1\}, b \in \{0, 3, 6\}\} = \{(0, 0, 0), (1, 0, 0), (0, 3, 0), (1, 3, 0), (0, 6, 0), (1, 6, 0)\}$$