The Fundamental Thm of Finite Abelian Groups

We are now in a position to give a complete classification of all finite Abelian groups.

The Fundamental Thm of Finite Abelian Gps
Every finite Abelian group is a direct product of cyclic groups of prime power order, uniquely determined up to the order in which the factors of the product are written. That is, if $G$ is a finite Abelian group, then there is a list of prime powers $p_1^{e_1}, p_2^{e_2}, \ldots, p_k^{e_k}$ (not necessarily distinct) so that

$$G \cong \mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{e_k}},$$

and this decomposition is unique up to permutation of the factors $\mathbb{Z}_{p_i^{e_i}}$.

Proof The proof is rather long, so we organize it into a series of lemmas:

**Lemma 1** Let $G$ be an Abelian group of order $m_1m_2$ where $m_1$ and $m_2$ are relatively prime, i.e., $\gcd(m_1,m_2) = 1$, and $m_1, m_2 > 1$. Then $G = H_1 \times H_2$ for $H_1 = \{x \in G \mid x^{m_1} = e\}$ and $H_2 = \{x \in G \mid x^{m_2} = e\}$. Further, $H_1$ has order $m_1$ and $H_2$ has order $m_2$.
To prove this, we first check that $H_1$ and $H_2$ are closed under the operation of $G$, hence are subgroups of the finite group $G$. Since $G$ is Abelian, $H_1$ and $H_2$ are normal in $G$. As $\gcd(m_1,m_2) = 1$, we can find integers $s$ and $t$ so that $1 = sm_1 + tm_2$. So for any $x \in G$, we can write $x = x^{sm_1+tm_2} = x^{sm_1}x^{tm_2}$; but $(x^{sm_1})^{m_2} = (x^s)^{m_2} = e \Rightarrow x^{sm_1} \in H_2$, and similarly, $x^{tm_2} \in H_1$. Therefore $G = H_1H_2$. Finally, $x \in H_1 \cap H_2 \Rightarrow x = x^{sm_1+tm_2} = (x^{m_1})^s(x^{m_2})^t = e$, so $H_1 \cap H_2 = \{e\}$. This proves that $G = H_1 \times H_2$. To show that $H_1$ has order $m_1$, we see that

$$m_1m_2 = |G| = |H_1H_2| = \frac{|H_1| \cdot |H_2|}{|H_1 \cap H_2|} = |H_1| \cdot |H_2|.$$ 

By Cauchy’s Theorem, every prime factor of $H_1$ gives rise to an element of $H_1$ having that order; but then that prime will have to divide $m_1$ as well. Similarly, every prime factor of $H_2$ is a prime factor of $m_2$ as well. But $m_1$ and $m_2$ are relatively prime, so they share no prime factors and by the last equation above, we must also have $|H_1| = m_1$ and $|H_2| = m_2$.

Now if the Abelian group $G$ has order $n$, and if $n$ has prime factorization $p_1^{e_1}p_2^{e_2} \cdots p_k^{e_k}$, then
m_1 = p_1^{e_1} and m_2 = p_2^{e_2} \cdots p_k^{e_k} satisfy the conditions of the lemma. So we can write G as the internal direct product of the subgroups

H_1 = \{x \in G \mid x^{m_1} = e\} and G_2 = \{x \in G \mid x^{m_2} = e\}.

Then we use the lemma to write G_2 as the internal direct product of its subgroups

H_2 = \{x \in G \mid x^{p_2^{e_2}} = e\}
and G_3 = \{x \in G \mid x^{p_3^{e_3} \cdots p_k^{e_k}} = e\}.

Continuing in this fashion, we obtain a factorization

G = H_1 \times H_2 \times \cdots \times H_k

of G as an internal direct product of the subgroups

H_i = \{x \in G \mid x^{p_i^{e_i}} = e\}. Each of the groups H_i is an Abelian group of prime power order p_i^{e_i}.

LEMMA 2 Let H be an Abelian group of prime power order p^e and suppose that a \in H is an element with maximal order. Then H has a subgroup K so that H = \langle a \rangle \times K.

The proof of this lemma is by induction on e. If e = 1, then a has order p and we take K to be the trivial subgroup: H = \langle a \rangle \times \langle e \rangle satisfies the conclusion of the Lemma.

If e > 1, then suppose that the Lemma holds true for all groups H whose orders are powers of p
smaller than $p^e$. Suppose now that $H$ has order $p^e$ and $a$ has order $p^m$. If $m = e$, then $a$ generates all of $H$, so as before $H = \langle a \rangle \times \langle e \rangle$. If $m < e$, then $\langle a \rangle \neq H$ and from the elements of $H$ not in $\langle a \rangle$ we choose an element $b$ of smallest order. We claim that $|b| = p$, for certainly $|b|$ is some power of $p$, but if it were larger than $p$, then $b^p$ would have order smaller than $b$ so that $b^p \in \langle a \rangle \Rightarrow b^p = a^q$. Also $(a^q)^{p^{m-1}} = b^{p^m} = e \Rightarrow |a^q| \leq p^{m-1}$. But then

$$\frac{p^e}{\gcd(p^e, q)} = |a| < p^e \Rightarrow p \text{ divides } q,$$

so we can write $q = pr$ and $b^p = a^q = a^{pr}$. Now the element $c = a^{-r}b$ is not in $\langle a \rangle$ (else $b$ would be), but

$c^p = (a^{-r}b)^p = a^{-q}b^p = e \Rightarrow |c| = p$. This violates the choice of $b$ as having minimal order among elements not in $\langle a \rangle$ unless $b$ also has order $p$.

Consider now the factor group $\overline{H} = H / \langle b \rangle$, whose elements we will denote for simplicity’s sake by overscoring its representative from $H$. For instance, we write $\overline{a}$ for the coset $a\langle b \rangle$. If $\overline{a}$ has order less than $p^m$ in $\overline{H}$, then

$$\overline{a}^{p^{m-1}} = e \Rightarrow \overline{a}^{p^{m-1}} \in \langle b \rangle \Rightarrow a^{p^{m-1}} \in \langle a \rangle \cap \langle b \rangle = \{e\}$$

so that $a$ could not have order $p^m$ in $H$. Thus the
order of $\sigma$ equals $p^m$, and so $\sigma$ has maximal order in $\mathcal{H}$. But $\mathcal{H}$ has order $|H|/p$, so by the induction hypothesis, $\mathcal{H} = \langle \sigma \rangle \times K$ for some subgroup $K$ of $\mathcal{H}$. Let $K$ be the pullback of $\bar{K}$ under the natural map from $H$ to $\mathcal{H}$ (that is, $K = \{k \in H \mid \bar{k} \in \bar{K}\}$). Then $\langle a \rangle \cap K = \{e\}$, for $x \in \langle a \rangle \cap K \Rightarrow x \in \langle \sigma \rangle \cap \bar{K} = \{e\} \Rightarrow x \in \langle a \rangle \cap \langle b \rangle = \{e\}$. Therefore, since $\bar{b} = e \in \bar{K}$, $|K| = |\bar{K}| \cdot p$ and

$$|\langle a \rangle K| = \frac{|a| \cdot |K|}{|\langle a \rangle \cap K|} = |a| \cdot |K| = |\sigma| \cdot |K| \cdot p = |H|/p = |H|$$

which implies that $H = \langle a \rangle K$, from which it follows that $H = \langle a \rangle \times K$.

Successive application of Lemma 2 allows us to assert

**Lemma 3** Let $H$ be an Abelian group of prime power order $p^e$. Then $H$ is an internal direct product of cyclic groups.

Combining this result with the result we derived above, that the finite Abelian group $G$ is an internal direct product of its subgroups of the form $H_i = \{x \in G \mid x^{p_{i}^{e_i}} = e\}$, each of which has prime power order, we know then that $G$ is an internal
direct product of cyclic groups of prime power order. We need only prove that the cyclic groups in this direct product decomposition are uniquely determined up to isomorphism and reordering within the product.

**LEMMA 4** Suppose that $G$ is a finite Abelian group of prime power order $p^e$. If $G = H_1 \times H_2 \times \cdots \times H_r$ and $G = K_1 \times K_2 \times \cdots \times K_s$, where the $H$'s and $K$'s are each nontrivial cyclic subgroups of $G$ whose orders satisfy $|H_1| \geq |H_2| \geq \cdots \geq |H_r|$, $|K_1| \geq |K_2| \geq \cdots \geq |K_s|$. Then $r = s$ and $|H_i| = |K_i|$ for every $i$.

This last lemma is proved by induction on $|G|$. The smallest case, $|G| = p$, is trivial. So suppose that $|G| > p$ and that the lemma holds for all finite Abelian groups of $p$-power order less than that of $G$. The subset $G^p = \{g \in G \mid g = x^p \text{ for some } x \in G\}$ is a subgroup of $G$, as it is clearly closed under the operation. Further, since $p$ is one of the prime factors of $|G|$, $G^p$ is a proper subgroup (since no element whose order in $G$ is a maximal power of $p$ lies in $G^p$). So let $p$ be a prime factor of $|G|$. Then $G^p = H_1^p \times H_2^p \times \cdots \times H_r^p$ and $G^p = K_1^p \times K_2^p \times \cdots \times K_s^p$, where $r'$ is the largest value of $i$ so that $|H_i| > p$ and $s'$ is the largest value of $i$ so that $|K_i| > p$. Since $|G^p| < |G|$, our induction hypothesis guarantees that $r' = s'$ and that $|H_i^p| = |K_i^p|$ for each
i. But also, $|H_i|^p = |H_i| \cdot p$ and $|K_i|^p = |K_i| \cdot p$. So $|H_i| = |K_i|$ for every $i = 1, 2, ..., r'$. But $|H_i| = p$ and $|K_i| = p$ for every $i > r'$ and

$$|H_1 \parallel H_2 \parallel \cdots \parallel H_r| \cdot p^{r-r'} = |H_1 \parallel H_2 \parallel \cdots \parallel H_r| = G$$

$$= |K_1 \parallel K_2 \parallel \cdots \parallel K_s|$$

$$= |K_1 \parallel K_2 \parallel \cdots \parallel K_s| \cdot p^{s-s'}$$

so in fact $r = s$ as well.

This completes the proof of the Fundamental Theorem. //
Examples:
A complete list of all Abelian groups of order 1176 up to isomorphism and rearrangement of terms is

\[ \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49} \]
\[ \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49} \]
\[ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49} \]
\[ \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7 \]
\[ \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7 \]
\[ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7 \]

In other words, there are six distinct isomorphism classes of Abelian groups of this order.
The subgroup of \( U(135) \) given by

\[ G = \{1,8,17,19,26,28,37,44,46,53,62,64,71,73,82,89,91,98,107,109,116,118,127,134\} \]

has order 24, so it is isomorphic to one of the three groups

\[ \mathbb{Z}_8 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{24} \]
\[ \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12} \oplus \mathbb{Z}_2 \]
\[ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \]

But \( 8^{12} = 1 \) and \( 8^6 = 109 \) in \( G \). So \( |8| = 12 \) while \( |134| = 2 = |109| \). As there is more than one element of order 2, \( G \) is not cyclic, so \( G \cong \mathbb{Z}_{12} \oplus \mathbb{Z}_2 \).
Corollary  Let $m$ divide the order of a finite Abelian group $G$ of order $n$. Then $G$ has a subgroup of order $m$.

Proof  If the prime factorization of $n$ is $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then the prime factorization of $m$ is $p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$ where $0 \leq d_i \leq e_i$ for each $i$. Since $G$ is isomorphic to an internal direct product of subgroups $H_i$, each of order $p_i^{e_i}$, we are done if we can show that each $H_i$ has a subgroup $K_i$ of order $p_i^{d_i}$, for then the internal direct product of these $K_i$ forms a subgroup of $G$ of order $m$. (Note that since the $H$'s have pairwise trivial intersection with each other in $G$, so must the $K$'s.)

In other words, we might as well assume that $n = p^e$ is a power of a single prime and that $m = p^d$ with $0 \leq d \leq e$. By Lemma 3, we can write $G = \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_r \rangle$ where each $g_i$ has order $p^{c_i}$, arranged here so that $c_1 \geq c_2 \geq \cdots \geq c_r$; note also that $c_1 + c_2 + \cdots + c_r = e$. Choose integers $b_1 \geq b_2 \geq \cdots \geq b_r$ with $b_i$ as large as possible so that $b_i \leq c_i$ and so that $b_1 + b_2 + \cdots + b_i \leq d$. This ensures that $b_i \leq c_i$ and $b_1 + b_2 + \cdots + b_r = d$. By putting $h_i = g_i^{p^{c_i-b_i}}$, we have that $|h_i| \equiv g_i^{p^{c_i-b_i}} \equiv p^{c_i} / p^{c_i-b_i} = p^{b_i}$. Thus, the subgroup $H = \langle h_1 \rangle \times \langle h_2 \rangle \times \cdots \times \langle h_r \rangle$ has order $p^{b_1} p^{b_2} \cdots p^{b_r} = p^{b_1+b_2+\cdots+b_r} = p^d = m$. //