The main goal of this section is to prove the following fact:

Theorem 16.1

If G is a finite abelian group then G is isomorphic to a direct product of cyclic groups whose orders are powers of primes:

$$G \cong \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \ldots \times \mathbb{Z}_{p_k^{r_k}}$$

for primes $p_1, \ldots, p_k$ and integers $r_1, \ldots, r_k \geq 1$ such that $p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_k^{r_k} = |G|$.

Example. Take $72 = 2^3 \cdot 3^2$. Theorem 16.1 says that every abelian group of order 72 is isomorphic to one of the following groups:

$$\begin{array}{ll}
\mathbb{Z}_8 \times \mathbb{Z}_9 & \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \\
\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9 & \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \\
\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 & \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3
\end{array}$$

Definition 16.2

A *short exact sequence* of groups is a sequence group homomorphisms

$$K \xrightarrow{i} G \xrightarrow{q} H$$

such that:

- i is 1-1
- q is onto
- $\mathrm{Im}(i) = \mathrm{Ker}(q)$

Example. Let K be a normal subgroup of G and let $i\colon K \to G$ be the inclusion homomorphism: $i(a) = a$. Also, let $q\colon G \to G/K$ be the quotient homomorphism $q(a) = aK$. This defines a short exact sequence

$$K \xrightarrow{i} G \xrightarrow{q} G/K$$

Example. If $f\colon G \to H$ is homomorphism which is onto, then we have a short exact sequence

$$\mathrm{Ker}(f) \xrightarrow{i} G \xrightarrow{f} H$$

where $i\colon \mathrm{Ker}(f) \to G$ is the inclusion homomorphism.

Example. Let G, H be groups. Define $i\colon G \to G \times H$ by $i(g) = (g, e)$, and $q\colon G \times H \to H$ by $q(g, h) = h$. This defines a short exact sequence

$$G \xrightarrow{i} G \times H \xrightarrow{q} H$$

Notice that in this case we also have a homomorphism $s\colon H \to H \times G$, $s(h) = (e, h)$ and $q \circ s = \mathrm{id}_H$.

Theorem 16.3

Consider a short exact sequence

$$K \xrightarrow{i} G \xrightarrow{q} H$$

where K, G, H are abelian groups. Assume that there exists a homomorphism $s\colon H \to G$ such that $q \circ s(h) = h$ for all $h \in H$. Then $G \cong K \times H$.

Note. Theorem 16.3 is not true in general for non-abelian groups. For example, in the dihedral group D_4 take the subgroup of rotations $K = \{I, R_{90}, R_{180}, R_{270}\}$. Since K is a normal subgroup of D_4, this gives a short exact sequence

$$K \xrightarrow{i} D_4 \xrightarrow{q} D_4/K$$

The group D_4/K consists of two cosets: IK and VK. Define $s\colon D_4/K \to D_4$ by $s(IK) = I$ and $s(VK) = V$. One can check that this is a group homomorphism. Moreover, $q(s(IK)) = IK$ and $q(s(VK)) = VK$. However, D_4 is not isomorphic to $K \times D_4/K$. Indeed, since $K \cong \mathbb{Z}_4$ and $D_4/K \cong \mathbb{Z}_2$, thus $K \times D_4/K \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ is an abelian group, while D_4 is non-abelian.

Proof of Theorem 16.3. Define a function $f\colon K \times H \to G$ by $f(k, h) = i(k) \cdot s(h)$. We will show that this function is an isomorphism of groups.

First, we check that f is a homomorphism:

$$\begin{aligned} f((k,h)\cdot(k',h')) &= f(kk',hh') \\ &= i(kk')\cdot s(hh') \\ &= i(k)\cdot i(k')\cdot s(h)\cdot s(h') \\ &= (i(k)\cdot s(h))\cdot(i(k')\cdot s(h')) \\ &= f(k,h)\cdot f(k',h') \end{aligned}$$

Next, assume that $(k,h)\in \mathrm{Ker}(f)$. Then $f(k,h)=i(k)\cdot s(h)=e$. This gives:

$$e = q(i(k)\cdot s(h)) = q(i(k))\cdot q(s(h)) = e\cdot h = h$$

so $e=h$. Thus, $e=f(k,h)=f(k,e)=i(k)\cdot e=i(k)$. Since i is 1-1, we get that $k=e$. Therefore the only element in $\mathrm{Ker}(f)$ is the identity element (e,e), which means that f is 1-1.

It remains to show that f is onto. Take an element $g\in G$, and let $h=q(g)$. We have

$$q(gs(h)^{-1}) = q(g)\cdot q(s(q(g^{-1}))) = q(g)\cdot q(g^{-1}) = e$$

which shows that $gs(h^{-1})\in\mathrm{Ker}(q)$. By exactness, we have $\mathrm{Ker}(q)=\mathrm{Im}(i)$, so there is an element $k\in K$ such that $i(k)=g\cdot s(h^{-1})$. Consider the element $(k,h)\in K\times H$. We have:

$$f(k,h) = i(k)\cdot s(h) = g\cdot s(h^{-1})\cdot s(h) = g$$

□

Corollary 16.4

Consider a short exact sequence

$$K \xrightarrow{i} G \xrightarrow{q} H$$

where K,G,H are abelian groups. Assume that there exists a homomorphism $s\colon H\to G$ such that $q\circ s$ is an isomorphism. Then $G\cong K\times H$.

Proof. Define $f=(q\circ s)^{-1}\circ q\colon G\to H$. The sequence

$$K \xrightarrow{i} G \xrightarrow{f} H$$

is a short exact sequence. Moreover, we have $f\circ s=(q\circ s)^{-1}\circ q\circ s=\mathrm{id}_H$. Thus by Theorem 16.3 we get $G\cong K\times H$. □

Theorem 16.5

Let G be a finite abelian group. Assume that $|G| = p^r m$ where p is a prime, $r \geq 1$ and m is a number which is not divisible by p. Then $G = K \times H$ where $|K| = p^r$ and $|H| = m$.

Lemma 16.6

Let G be a finite abelian group. Assume that there exists a prime p such that the order of each element $g \in G$ is a power of p. For $m \in \mathbb{Z}$ consider the function

$$f\colon G \to G$$

given by $f(g) = g^m$. If m is not divisible by p then f is a group isomorphism.

Proof. By Corollary 15.8 we have $|G| = p^r$ for some $r \geq 0$. Therefore $g^{p^r} = e$ for all $g \in G$.

Since $\gcd(m, p^r) = 1$, there exist $k, l \in \mathbb{Z}$ such that $km + lp^r = 1$. Define $s\colon G \to G$ by $s(g) = g^k$. We have

$$s \circ f(g) = (g^m)^k = g^{km} = g^{1-lp^r} = g \cdot g^{-lp^r} = ge = g$$

so $s \circ f = \mathrm{id}_G$. Similarly, $f \circ s = \mathrm{id}_G$. Thus f is an isomorphism and $f^{-1} = s$. $\square$

Proof of Theorem 16.5. Define

$$H := \{g \in G \mid \ |g| = p^i \text{ for some } i \geq 1\}$$

One can check that this is a subgroup of G. Notice that if $g \in G$ then $g^m \in H$. Indeed, we have

$$(g^m)^{p^r} = g^{mp^r} = g^{|G|} = e$$

so $|g^m|$ divides p^r. As a consequence we obtain a homomorphim $q\colon G \to H$, $q(g) = g^m$. This homomorphism is onto since, by Lemma 16.6, $q|_H\colon H \to H$ is an isomorphism. Take the short exact sequence

$$\mathrm{Ker}(q) \longrightarrow G \xrightarrow{q} H$$

Define $s\colon H \to G$ by $s(h) = h$. The composition $q \circ s\colon H \to H$ is given by $q \circ s(h) = h^m$ which is an isomorphism by Lemma 16.6. Using Corollary 16.4 we obtain that $G \cong \mathrm{Ker}(q) \times H$.

We have $|H| \cdot |\mathrm{Ker}(q)| = |G| = p^r m$. By Corollary 15.8, $|H|$ is a power of p. Also, since $\mathrm{Ker}(q) = \{g \in G \mid g^m\}$, thus the order of every element of $\mathrm{Ker}(q)$ divides m. This implies that $\mathrm{Ker}(q)$ does not contain any elements of order p. By Cauchy Theorem 15.6, we obtain that $|\mathrm{Ker}(q)|$ is not divisible by p. Therefore $|H| = p^r$ and $|\mathrm{Ker}(q)| = m$. $\square$

Corollary 16.7

If G is a finite abelian group and $|G| = p_1^{r_1} p_2^{r_2} \cdot \ldots \cdot p_k^{r_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes then

$$G = G_1 \times G_2 \times \ldots \times G_k$$

where $|G_i| = p_i^{r_i}$.

Proof. We use induction with respect to the number of distinct primes k. If $k = 1$ then $|G| = p_1^{r_1}$, so we take $G_1 = G$.

Assume that the statement is true for all abelian groups whose order is a product of powers of k distinct primes, and let G be a group such that

$$|G| = p_1^{r_1} p_2^{r_2} \cdot \ldots \cdot p_k^{r_k} p_{k+1}^{r_{k+1}}$$

where $p_1, \ldots, p_{k+1}$ are distinct primes. By Theorem 16.5 we get $G = G_1 \times H$ where $|G_1| = p_1^{r_1}$ and $|H| = p_2^{r_2} \cdot \ldots \cdot p_k^{r_k} p_{k+1}^{r_{k+1}}$ By the inductive assumption, $H \cong G_2 \times \ldots \times G_{k+1}$ where $|G_i| = p_i^{r_i}$. This gives

$$G \cong G_1 \times H \cong G_1 \times G_2 \times \ldots \times G_{k+1}$$

$\square$

Theorem 16.8

If G is an abelian group such that $|G| = p^n$ for some prime p then G is a direct product of cyclic groups:

$$G \cong \mathbb{Z}_{p^{k_1}} \times \mathbb{Z}_{p^{k_2}} \times \ldots \times \mathbb{Z}_{p^{k_m}}$$

for some $k_1, k_2, \ldots, k_m$.

Idea of Proof. Use induction with respect to the order of the group G. Let p^r be the largest order of an element in G, and let $a \in G$ be an element such that $|a| = p^r$.

One can show that there exists a short exact sequence

$$K \xrightarrow{i} G \xrightarrow{q} \mathbb{Z}_{p^r}$$

such that $q(a) = 1 \in \mathbb{Z}_{p^r}$. Take the homomorphism $s\colon \mathbb{Z}_{p^r} \to G$ given by $s(k) = a^k$. Since $q \circ s(k) = k$ for all $k \in \mathbb{Z}^{p^r}$, by Theorem 16.3 we obtain that $G \cong \mathbb{Z}_{p^r} \times K$. By the inductive assumption we get that K is a direct product of cyclic groups, $K \cong \mathbb{Z}_{p^{k_1}} \times \ldots \times \mathbb{Z}_{p^{k_m}}$, which gives $G \cong \mathbb{Z}_{p^r} \times (\mathbb{Z}_{p^{k_1}} \times \ldots \times \mathbb{Z}_{p^{k_m}})$. $\square$

Proof of Theorem 16.1. It follows from Corollary 16.7 and Theorem 16.8. $\square$