EXERCISE 1. Let H be a finite cyclic group, so $\widehat{H} \simeq H$, so $\widehat{H}$ is also cyclic, so $\widehat{H} = \langle \psi \rangle$ for some character ψ. Prove that $\ker \psi = 1$.

THM A. (Splitting Theorem) Let G be a finite abelian group, and let H be a cyclic subgroup of maximal order. Then $G = H \times K$ for some subgroup K, i.e. G splits into an internal direct product of H and K.

Proof. Let $H = \langle h \rangle$ and let $m = |H|$, so h is an element of order m, which is the largest order of any element in G. By Exercise 1, $\widehat{H} = \langle \psi \rangle$ where ψ is a character of H of order m, and $\ker \psi = 1$. By THM E in §14, ψ extends to a character χ of G.

Let n be the order of χ. Then $\chi^n = 1$, i.e. $\chi(g)^n = 1$ for all $g \in G$, so $\psi(g)^n = 1$ for all $g \in H$, i.e. $\psi^n = 1$, so $m | n$, so $m \leq n$.

Since $\chi(G)$ is a finite subgroup of $\mathbb{C}$, $\chi(G)$ is cyclic, by THM B in §14. Choose $g \in G$ so that $\chi(G) = \langle \chi(g) \rangle$. Since $\chi^k \neq 1$ for $0 < k < n$, it follows that $\chi(g^k) = \chi(g)^k \neq 1$ for $0 < k < n$, so $g^k \neq 1$ for $0 < k < n$, so g has order $\geq n$, so $\boxed{m \geq n}$.
Combining $\bigcirc$ and $\square$ gives $m = n$, i.e.

$$\checkmark \qquad |H| = |\chi(G)|.$$

Let $K = \ker \chi$. Then $H \cap K = \ker \psi$, and $\ker \psi = 1$, as shown above, so

$$* \qquad H \cap K = 1.$$

We have

$$H \simeq H/1 \overset{\text{by } *}{=} H/(H\cap K) \overset{\text{2nd isom.}}{\simeq} HK/H \subseteq G/K \overset{\text{1st isom.}}{\simeq} \chi(G),$$

so by $\checkmark$ the $\subseteq$ must be $=$, so

$$** \qquad HK = G.$$

Combining $*$ & $**$ gives $G = H \times K$, by THM B in §13.

LEMMA. (1) The direct product of abelian groups is abelian.
(2) If H and K are finite abelian groups, then $\widehat{H\times K} \simeq \hat{H}\times\hat{K}$.

EXERCISE 2. Prove the Lemma. Hint for (2). For $\varphi\in\hat{H}$ and $\psi\in\hat{K}$, define $\varphi\times\psi: H\times K\to C$ by $(\varphi\times\psi)(h,k)=\varphi(h)\psi(k)$. Prove that $\varphi\times\psi\in\widehat{H\times K}$ and that the map which sends φ,ψ to $\varphi\times\psi$ is an isomorphism from $\hat{H}\times\hat{K}$ to $\widehat{H\times K}$.

COR 1 (Duality Theorem) Each finite abelian group G is isomorphic to its character group $\hat{G}$:

$$\boxed{\hat{G}\simeq G}$$

REMARK We know some of this already. We know $\hat{G}\simeq G$ for each finite cyclic group by THM D in §14, and we know $|\hat{G}|=|G|$ for each finite abelian group by THM G in §14. There are still things to do, since not every finite abelian group is cyclic, e.g. $C_2\times C_2$, of order 4, is not cyclic, since its elements have order 1 or 2 (& not 4).

Pf of THM B. If $|G|=1$, then $|\hat{G}|=1$, so $\hat{G}\simeq G$ (groups of order 1 are isomorphic). If $|G|>1$, let H be a cyclic subgroup of maximal order. We have $|H|>1$. By THM A, $G=H\times K$ for some subgroup K of G. We have $|K|<|G|$, so by induction on order, $\hat{K}\simeq K$. By THM D in §14, $\hat{H}\simeq H$. Using the Lemma,

$$\hat{G}=\widehat{H\times K}\simeq\hat{H}\times\hat{K}\simeq H\times K=G.$$

DEF. Let $H_1,\dots,H_r$ be groups. The external direct product $H_1\times\cdots\times H_r$ is the cartesian product of $H_1,\dots,H_r$, i.e. the set of all r-tuples $(h_1,\dots,h_r)$ with $h_1\in H_1,\dots,h_r\in H_r$, with componentwise multiplication, clearly making $H_1\times\cdots\times H_r$ into a group. If $H_1,\dots,H_r$ are finite, clearly $|H_1\times\cdots\times H_r|=|H_1|\cdots|H_r|$.

COR 2 (Basis Theorem) Each finite abelian group is isomorphic to a direct product of cyclic groups

Proof. Let G be a finite abelian group. If $|G|=1$, we agree to regard G as a direct product of no cyclic groups. If $|G|>1$, let H_1 be a cyclic subgroup of maximal order. Then $|H_1|>1$, and by THM A, we have $G=H_1\times K$ for some subgroup K with $|K|<|G|$.
By induction on order, K is isomorphic to a direct product of cyclic groups $H_2,\dots,H_r$:

$$K\simeq H_2\times\cdots\times H_r,$$

so

$$G=H_1\times K\simeq H_1\times H_2\times\cdots\times H_r.$$

DEF A *prime power* is any positive integer of the form p^q with p prime and $q\in\{0,1,2,\dots\}$.
Thus the first few prime powers are

$$1,2,3,4,5,7,8,9,11,13,16,17,\dots$$

THM B. Each finite abelian group is isomorphic to a direct product of cyclic groups of prime power orders >1.

EXAMPLES $C_6\simeq C_2\times C_3$, $C_{60}\simeq C_{2^2}\times C_3\times C_5$, $C_2\times C_{30}=C_2\times C_2\times C_3\times C_5$

Proof. It suffices by COR 2 to show that each finite cyclic group is isomorphic to a direct product of cyclic groups of prime power orders >1.

Using THM C in §13 we see that for $m,n\in\mathbb{N}$ with $(m,n)=1$,

$$C_{mn}\simeq C_m\times C_n$$

It follows from this that for powers $p_1^{\nu_1},\dots,p_r^{\nu_r}$ of distinct primes,

$$C_{p_1^{\nu_1}\cdots p_r^{\nu_r}}\simeq C_{p_1^{\nu_1}}\times\cdots\times C_{p_r^{\nu_r}}.$$

REMARK The representation of a finite abelian group as an internal direct product of cyclic groups of prime power order is not unique. For example, there are 3 different subgroups H_1,H_2,H_3 of order 2 in $C_2\times C_2$, and $C_2\times C_2=H_1\times H_2=H_1\times H_3=H_2\times H_3$.

THM C Let G be a finite abelian group, and let $G = H_1 \times \cdots \times H_r$ with each H_j cyclic of prime power order > 1. Then for each prime power p^c, the number of $j \in \{1,\dots,r\}$ for which $|H_j| = p^c$ is determined by G and p^c

Proof. The general case may be reduced easily to the special case in which $|G| = p^a$, which we will assume. Thus $|H_j| = p^{b_j}$ for $j = 1,\dots,r$ and our job is to show that the number of j for which $b_j = c$ is determined by G and c.

Let $g = (h_1, \dots, h_r) \in G$. For each integer $c \geq 0$, we have

$$g^{p^c} = 1 \iff h_j^{p^c} = 1 \quad \forall j \in \{1,\dots,r\},$$

so

$$|\{g \in G : g^{p^c} = 1\}| = \prod_{j=1}^{r} |\{h_j \in H_j : h_j^{p^c} = 1\}| \circleddash \prod_{j=1}^{r} p^{\min\{b_j, c\}},$$

with $\circleddash$ because in a cyclic group of order p^b the number of elements of order $| p^c$ is $p^{\min\{b,c\}}$.

$$(1) \quad \sum_{j=1}^{r} \min\{b_j, c\} \text{ is determined by } G \text{ and } c.$$

little lemma: for $b, c \in \mathbb{N}$, $\min\{b,c\} - \min\{b, c-1\} = \begin{cases} 0 & \text{for } b < c \\ 1 & \text{for } b \geq c \end{cases}$.

proof: For $b < c$, each min is b, while for $b \geq c$ the mins are c and $c-1$.

By (1) and the little lemma,

$$(2) \quad \sum_{\substack{j=1 \\ b_j \geq c}}^{r} 1 \left(= \sum_{j=1}^{r} \min\{b_j, c\} - \sum_{j=1}^{r} \min\{b_j, c-1\} \right) \text{ is determined by } G \text{ and } c.$$

From (2) it follows that

$$\sum_{\substack{j=1 \\ b_j = c}}^{r} 1 \left(= \sum_{\substack{j=1 \\ b_j \geq c}}^{r} 1 - \sum_{\substack{j=1 \\ b_j \geq c+1}}^{r} 1 \right) \text{ is determined by } G \text{ and } c.$$

EXERCISE 3. denote by $N_a(n)$ the number of nonisomorphic abelian groups of order n. Prove that $N_a(mn) = N_a(m) N_a(n)$ for $m, n \in \mathbb{N}$ with $(m,n) = 1$.

EXERCISE 4. Prove that for each $c \in \mathbb{N}$ and each prime p, $N_a(p^c)$ is equal to the number of (finite) sequences of positive integers $b_1, \ldots, b_r$ for which

$$b_1 \geq b_2 \geq \cdots \geq b_r$$

and

$$c = b_1 + b_2 + \cdots + b_r$$

EXAMPLE Abelian groups of order $32 = 2^5$. $N_a(32) = 7$.

$5 = 5$	C_{32}
$= 4+1$	$C_{16} \times C_2$
$= 3+2$	$C_8 \times C_4$
$= 3+1+1$	$C_8 \times C_2 \times C_2$
$= 2+2+1$	$C_4 \times C_4 \times C_2$
$= 2+1+1+1$	$C_4 \times C_2 \times C_2 \times C_2$
$= 1+1+1+1+1$	$C_2 \times C_2 \times C_2 \times C_2 \times C_2$

Each abelian group of order 32 is isomorphic to exactly one group in this list.

EXAMPLE By Exercises 3 and 4, and we see that $N_a(144) = N_a(2^4 3^2) = 5 \cdot 2 = 10$

$4 = 4$	$2 = 2$
$= 3+1$	$= 1+1$
$= 2+2$	
$= 2+1+1$	
$= 1+1+1+1$	

EXERCISE 5 True or False:
(0) Any two abelian groups of order 4 are isomorphic
(1) Any two groups of order 5 are isomorphic
(2) Any two abelian groups of order 6 are isomorphic.
(3) Any two groups of order 6 are isomorphic.

It is much harder to determine, even for relatively small n, the number $N(n)$ of nonisomorphic groups of order n (including the nonabelian ones). From the very large book of Hall and Senior, I quote:

n	1	2	4	8	16	32	64
$N(n)$	1	1	2	5	14	51	267