(a) $r \geq 0$ and $n_j \geq 2$ for all j, and

(b) $n_{i+1} \mid n_i$ for $1 \leq i \leq s-1$

(2) the expression in (1) is unique: if $G \cong \mathbb{Z}^t \times Z_{m_1} \times Z_{m_2} \times \cdots \times Z_{m_u}$, where t and $m_1, m_2, \ldots, m_u$ satisfy (a) and (b) (i.e., $t \geq 0$, $m_j \geq 2$ for all j and $m_{i+1} \mid m_i$ for $1 \leq i \leq u-1$), then $t = r$, $u = s$ and $m_i = n_i$ for all i.

Proof: We shall derive this theorem in Section 12.1 as a consequence of a more general classification theorem. For finite groups we shall give an alternate proof at the end of Section 6.1.

Definition. The integer r in Theorem 3 is called the *free rank* or *Betti number* of G and the integers $n_1, n_2, \ldots, n_s$ are called the *invariant factors* of G. The description of G in Theorem 3(1) is called the *invariant factor decomposition* of G.

Theorem 3 asserts that the free rank and (ordered) list of invariant factors of an abelian group are uniquely determined, so that two finitely generated abelian groups are isomorphic if and only if they have the same free rank and the same list of invariant factors. Observe that a finitely generated abelian group is a finite group if and only if its free rank is zero.

The order of a finite abelian group is just the product of its invariant factors (by Proposition 1). If G is a finite abelian group with invariant factors $n_1, n_2, \ldots, n_s$, where $n_{i+1} \mid n_i$, $1 \leq i \leq s-1$, then G is said to be of *type* $(n_1, n_2, \ldots, n_s)$.

Theorem 3 gives an effective way of listing *all* finite abelian groups of a given order. Namely, to find (up to isomorphism) all abelian groups of a given order n one must find all finite sequences of integers $n_1, n_2, \ldots, n_s$ such that

(1) $n_j \geq 2$ for all $j \in \{1, 2, \ldots, s\}$,
(2) $n_{i+1} \mid n_i$, $1 \leq i \leq s-1$, and
(3) $n_1 n_2 \cdots n_s = n$.

Theorem 3 states that there is a bijection between the set of such sequences and the set of isomorphism classes of finite abelian groups of order n (where each sequence corresponds to the list of invariant factors of a finite abelian group).

Before illustrating how to find all such sequences for a specific value of n we make some general comments. First note that $n_1 \geq n_2 \geq \cdots \geq n_s$, so n_1 is the largest invariant factor. Also, by property (3) each n_i divides n. If p is any prime divisor of n then by (3) we see that p must divide n_i for some i. Then, by (2), p also divides n_j for all $j \leq i$. It follows that

every prime divisor of n must divide the first invariant factor n_1.

In particular, if n is the product of distinct primes (all to the first power)[1] we see that $n \mid n_1$, hence $n = n_1$. This proves that if n is squarefree, there is only one possible list of invariant factors for an abelian group of order n (namely, the list $n_1 = n$):

[1] Such integers are called *squarefree* since they are not divisible by any square > 1.

Corollary 4. If n is the product of distinct primes, then up to isomorphism the only abelian group of order n is the cyclic group of order n, Z_n.

The factorization of n into prime powers is the first step in determining all possible lists of invariant factors for abelian groups of order n.

Example

Suppose $n = 180 = 2^2 \cdot 3^2 \cdot 5$. As noted above we must have $2 \cdot 3 \cdot 5 \mid n_1$, so possible values of n_1 are

$$n_1 = 2^2 \cdot 3^2 \cdot 5, \quad 2^2 \cdot 3 \cdot 5, \quad 2 \cdot 3^2 \cdot 5, \quad \text{or} \quad 2 \cdot 3 \cdot 5.$$

For each of these one must work out all possible n_2's (subject to $n_2 \mid n_1$ and $n_1 n_2 \mid n$). For each resulting pair n_1, n_2 one must work out all possible n_3's etc. until all lists satisfying (1) to (3) are obtained.

For instance, if $n_1 = 2 \cdot 3^2 \cdot 5$, the only number n_2 dividing n_1 with $n_1 n_2$ dividing n is $n_2 = 2$. In this case $n_1 n_2 = n$, so this list is complete: $2 \cdot 3^2 \cdot 5$, 2. The abelian group corresponding to this list is $Z_{90} \times Z_2$.

If $n_1 = 2 \cdot 3 \cdot 5$, the only candidates for n_2 are $n_2 = 2, 3$ or 6. If $n_2 = 2$ or 3, then since $n_3 \mid n_2$ we would necessarily have $n_3 = n_2$ (and there must be a third term in the list by property (3)). This leads to a contradiction because $n_1 n_2 n_3$ would be divisible by 2^3 or 3^3 respectively, but n is not divisible by either of these numbers. Thus the only list of invariant factors whose first term is $2 \cdot 3 \cdot 5$ is $2 \cdot 3 \cdot 5$, $2 \cdot 3$. The corresponding abelian group is $Z_{30} \times Z_6$.

Similarly, all permissible lists of invariant factors and the corresponding abelian groups of order 180 are easily seen to be the following:

Invariant Factors	Abelian Groups
$2^2 \cdot 3^2 \cdot 5$	Z_{180}
$2 \cdot 3^2 \cdot 5$, 2	$Z_{90} \times Z_2$
$2^2 \cdot 3 \cdot 5$, 3	$Z_{60} \times Z_3$
$2 \cdot 3 \cdot 5$, $2 \cdot 3$	$Z_{30} \times Z_6$

The process we carried out above was somewhat *ad hoc*, however it indicates that the determination of lists of invariant factors of all abelian groups of a given order n relies strongly on the factorization of n. The following theorem (which we shall see is equivalent to the Fundamental Theorem in the case of finite abelian groups) gives a more systematic and computationally much faster way of determining all finite abelian groups of a given order. More specifically, if the factorization of n is

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

it shows that all permissible lists of invariant factors for abelian groups of order n may be determined by finding permissible lists for groups of order $p_i^{\alpha_i}$ for each i. For a prime power, p^α, we shall see that the problem of determining all permissible lists is equivalent to the determination of all partitions of α (and does not depend on p).

Theorem 5. Let G be an abelian group of order $n > 1$ and let the unique factorization of n into distinct prime powers be

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Then

(1) $G \cong A_1 \times A_2 \times \cdots \times A_k$, where $|A_i| = p_i^{\alpha_i}$

(2) for each $A \in \{A_1, A_2, \ldots, A_k\}$ with $|A| = p^{\alpha}$,

$$A \cong Z_{p^{\beta_1}} \times Z_{p^{\beta_2}} \times \cdots \times Z_{p^{\beta_t}}$$

with $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_t \geq 1$ and $\beta_1 + \beta_2 + \cdots + \beta_t = \alpha$ (where t and $\beta_1, \ldots, \beta_t$ depend on i)

(3) the decomposition in (1) and (2) is unique, i.e., if $G \cong B_1 \times B_2 \times \cdots \times B_m$, with $|B_i| = p_i^{\alpha_i}$ for all i, then $B_i \cong A_i$ and B_i and A_i have the same invariant factors.

Definition. The integers p^{β_j} described in the preceding theorem are called the *elementary divisors* of G. The description of G in Theorem 5(1) and 5(2) is called the *elementary divisor decomposition* of G.

The subgroups A_i described in part (1) of the theorem are the Sylow p_i-subgroups of G. Thus (1) says that G is isomorphic to the direct product of its Sylow subgroups (note that they are normal — since G is abelian — hence unique). Part 1 is often referred to as *The Primary Decomposition Theorem* for finite abelian groups.[2] As with Theorem 3, we shall prove this theorem later.

Note that for p a prime, $p^{\beta} \mid p^{\gamma}$ if and only if $\beta \leq \gamma$. Furthermore, $p^{\beta_1} \cdots p^{\beta_t} = p^{\alpha}$ if and only if $\beta_1 + \cdots + \beta_t = \alpha$. Thus the decomposition of A appearing in part (2) of Theorem 5 is the invariant factor decomposition of A with the "divisibility" conditions on the integers p^{β_j} translated into "additive" conditions on their exponents. The *elementary divisors* of G are now seen to be the *invariant factors of the Sylow p-subgroups* as p runs over all prime divisors of G.

By Theorem 5, in order to find all abelian groups of order $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ one must find for each i, $1 \leq i \leq k$, all possible lists of invariant factors for groups of order $p_i^{\alpha_i}$. The set of elementary divisors of each abelian group is then obtained by taking one set of invariant factors from each of the k lists. The abelian groups are the direct products of the cyclic groups whose orders are the elementary divisors (and distinct lists of elementary divisors give nonisomorphic groups). The advantage of this process over the one described following Theorem 2 is that it is easier to systematize how to obtain all possible lists of invariant factors, $p^{\beta_1}, p^{\beta_2}, \ldots, p^{\beta_t}$, for a group of prime power order p^{β}. Conditions (1) to (3) for invariant factors described earlier then become

(1) $\beta_j \geq 1$ for all $j \in \{1, 2, \ldots, t\}$,

(2) $\beta_i \geq \beta_{i+1}$ for all i, and

(3) $\beta_1 + \beta_2 + \cdots + \beta_t = \beta$.

[2] Recall that for abelian groups the Sylow p-subgroups are sometimes called the p-primary components

Hence, each list of invariant factors in this case is simply a *partition* of β (ordered in descending order). In particular, the number of nonisomorphic abelian groups of order p^β (= the number of distinct lists) equals the number of partitions of β. This number is independent of the prime p. For example the number of abelian groups of order p^5 is obtained from the list of partitions of 5:

Invariant Factors	Abelian Groups
5	Z_{p^5}
4, 1	$Z_{p^4} \times Z_p$
3, 2	$Z_{p^3} \times Z_{p^2}$
3, 1, 1	$Z_{p^3} \times Z_p \times Z_p$
2, 2, 1	$Z_{p^2} \times Z_{p^2} \times Z_p$
2, 1, 1, 1	$Z_{p^2} \times Z_p \times Z_p \times Z_p$
1, 1, 1, 1, 1	$Z_p \times Z_p \times Z_p \times Z_p \times Z_p$

Thus there are precisely 7 nonisomorphic groups of order p^5, the first in the list being the cyclic group, Z_{p^5}, and the last in the list being the elementary abelian group, E_{p^5}.

If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ and q_i is the number of partitions of α_i, we see that the number of (distinct, nonisomorphic) abelian groups of order n equals $q_1 q_2 \cdots q_k$.

Example

If $n = 1800 = 2^3 3^2 5^2$ we list the abelian groups of this order as follows:

Order p^β	Partitions of β	Abelian Groups
2^3	3; 2, 1; 1, 1, 1	Z_8, $Z_4 \times Z_2$, $Z_2 \times Z_2 \times Z_2$
3^2	2; 1, 1	Z_9, $Z_3 \times Z_3$
5^2	2; 1, 1	Z_{25}, $Z_5 \times Z_5$

We obtain the abelian groups of order 1800 by taking one abelian group from each of the three lists (right hand column above) and taking their direct product. Doing this in all possible ways gives all isomorphism types:

$Z_8 \times Z_9 \times Z_{25}$
$Z_8 \times Z_9 \times Z_5 \times Z_5$
$Z_8 \times Z_3 \times Z_3 \times Z_{25}$
$Z_8 \times Z_3 \times Z_3 \times Z_5 \times Z_5$
$Z_4 \times Z_2 \times Z_9 \times Z_{25}$
$Z_4 \times Z_2 \times Z_9 \times Z_5 \times Z_5$
$Z_4 \times Z_2 \times Z_3 \times Z_3 \times Z_{25}$
$Z_4 \times Z_2 \times Z_3 \times Z_3 \times Z_5 \times Z_5$
$Z_2 \times Z_2 \times Z_2 \times Z_9 \times Z_{25}$
$Z_2 \times Z_2 \times Z_2 \times Z_9 \times Z_5 \times Z_5$
$Z_2 \times Z_2 \times Z_2 \times Z_3 \times Z_3 \times Z_{25}$
$Z_2 \times Z_2 \times Z_2 \times Z_3 \times Z_3 \times Z_5 \times Z_5$.

By the Fundamental Theorems above, this is a *complete list* of all abelian groups of order 1800 — every abelian group of this order is isomorphic to precisely one of the groups above and no two of the groups in this list are isomorphic.

We emphasize that the elementary divisors of G are not invariant factors of G (but invariant factors of *subgroups* of G). For instance, in case 1 above the elementary divisors 8, 9, 25 do not satisfy the divisibility criterion of a list of invariant factors.