16A. Direct products and Classification of Finite Abelian Groups

16A.1. Direct products.

Definition. Let $G$ and $H$ be groups. Their direct product is the group $G \times H$ defined as follows. As a set $G \times H = \{(g, h) : g \in G, h \in H\}$ is just the usual Cartesian product of $G$ and $H$ (the set of ordered pairs where the first component lies in $G$ and the second component lies in $H$). The group operation on $G \times H$ is defined by the formula

$$(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2) \text{ for all } g_1, g_2 \in G \text{ and } h_1, h_2 \in H.$$ 

Here $g_1g_2$ is the product of $g_1$ and $g_2$ in $G$ and $h_1h_2$ is the product of $h_1$ and $h_2$ in $H$.

Verification of group axioms for $G \times H$ is straightforward. The identity element of $G \times H$ is the pair $(e_G, e_H)$ where $e_G$ is the identity element of $G$ and $e_H$ is the identity element of $H$. Inverses in $G \times H$ are given by the formula

$$(g, h)^{-1} = (g^{-1}, h^{-1}).$$

The above definition easily generalizes to the case of more than 2 groups. Given any finite sequence of groups $G_1, \ldots, G_k$, we define their direct product $G_1 \times \ldots \times G_k$ to be the set of all $k$-tuples $(g_1, \ldots, g_k)$ with $g_i \in G_i$ for all $i$, with group operation defined by

$$(g_1, \ldots, g_k)(g'_1, \ldots, g'_k) = (g_1g'_1, \ldots, g_kg'_k) \text{ where } g_i, g'_i \in G_i \text{ for all } i.$$ 

Lemma 16A.1. The following hold:

(a) For any two groups $G$ and $H$, the direct products $G \times H$ and $H \times G$ are isomorphic. More generally, if $G_1, \ldots, G_k$ are any groups and $i_1, \ldots, i_k$ is any permutation of $1, \ldots, k$, then

$$G_1 \times \ldots \times G_k \cong G_{i_1} \times \ldots \times G_{i_k}.$$ 

(b) For any three groups $G, H$ and $K$ the groups $G \times H \times K$ and $G \times (H \times K)$ are isomorphic. More generally, for any sequence of groups $G_1, \ldots, G_k$ we have $G_1 \times G_2 \times \ldots \times G_k \cong G_1 \times (G_2 \times \ldots \times G_k)$.

Sketch of proof. (a) Define $\varphi : G \times H \to H \times G$ by $\varphi((g, h)) = (h, g)$. Then $\varphi$ is clearly bijective, and it is straightforward to check that $\varphi$ preserves the group operation. In the more general setting an isomorphism between
$G_1 \times \ldots \times G_k$ and $G_{i_1} \times \ldots \times G_{i_k}$ is given by the formula $\varphi((g_1, \ldots, g_k)) = (g_{i_1}, \ldots, g_{i_k})$.

(b) Similarly to (a), the map $\varphi : G \times H \times K \to G \times (H \times K)$ given by $\varphi((g, h, k)) = (g, (h, k))$ is an isomorphism. More generally, the map $\varphi : G_1 \times G_2 \times \ldots \times G_k \to G_1 \times (G_2 \times \ldots \times G_k)$ given by $\varphi((g_1, g_2, \ldots, g_k)) = (g_1, (g_2, \ldots, g_k))$ is an isomorphism. □

If $G_1, \ldots, G_k$ are finite groups, the order of their direct product is equal to the product of the orders:

(16A.1) $|G_1 \times G_2 \times \ldots \times G_k| = |G_1| \cdot |G_2| \cdot \ldots \cdot |G_k|.$

Indeed, if we want to construct an element of $G_1 \times \ldots \times G_k$, we have $|G_1|$ choices for the first component, $|G_2|$ choices for the second component etc. and finally $|G_k|$ choices for the $k$th component. Since choices at each step are made independently, the total number of choices is $|G_1| \cdot |G_2| \cdot \ldots \cdot |G_k|$.

16A.2. **Classification Theorem of Finite Abelian Groups.** If $G_1, \ldots, G_k$ are abelian groups, it is clear from the definition that their direct product $G_1 \times \ldots \times G_k$ is also abelian. In particular, given any integers $n_1, \ldots, n_k$ with $n_i \geq 2$ for all $i$, the direct product $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$ is abelian (as usual by $\mathbb{Z}_n$ we mean $\mathbb{Z}_n$ with respect to addition). It turns out that every finite abelian group is isomorphic to a group of this form.

**Theorem 16A.2** (Fundamental Theorem of Finite Abelian Groups, weak form). Let $G$ be a finite abelian group with $|G| \geq 2$. Then there exist integers $n_1, \ldots, n_k$ such that $G \cong \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$.

Later in the lecture we will refine the above statement, in particular, adding a suitable uniqueness part. Let us see some immediate applications of this Theorem to classification of abelian groups of small order.

**Example 1.** Let $G$ be an abelian group of order 4. Since $|\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}| = n_1 \ldots n_k$ by (16A.1) and the only ways to write 4 as a product of integers $\geq 2$ are 4 itself and 2·2, Theorem 16A.2 implies that $G$ must be isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

**Remark:** In Lecture 18 we will show (using a different argument) that actually every group of order 4 is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$, so in particular, every group of order 4 is abelian.

Recall that in Lecture 13 we have considered two abelian groups of order 4 which do not appear in the form $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$, namely $\mathbb{Z}_5^\times = \{[1], [2], [3], [4]\}$ (invertible elements of $\mathbb{Z}_5$ with respect to multiplication)
and \( \mathbb{Z}_8^x = \{[1],[3],[5],[7]\} \). By the above argument each of those groups must be isomorphic to \( \mathbb{Z}_4 \) or \( \mathbb{Z}_2 \times \mathbb{Z}_2 \), but which one?

We claim that \( \mathbb{Z}_5 \times \mathbb{Z}_8 \simeq \mathbb{Z}_4 \) while \( \mathbb{Z}_5 \times \mathbb{Z}_8 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \). Indeed, as verified in Lecture 13, \( \mathbb{Z}_5 \) is cyclic, hence \( \mathbb{Z}_5 \times \mathbb{Z}_8 \simeq \mathbb{Z}_4 \) by Theorem 15.2. On the other hand (again by Lecture 13), \( \mathbb{Z}_5 \times \mathbb{Z}_8 \) is not cyclic, so it cannot be isomorphic to \( \mathbb{Z}_4 \) (since a group isomorphic to a cyclic group must be cyclic). Therefore, \( \mathbb{Z}_5 \times \mathbb{Z}_8 \) must be isomorphic to \( \mathbb{Z}_2 \times \mathbb{Z}_2 \).

**Example 2.** Let \( G \) be an abelian group of order 6. As in previous example, by Theorem 16A.2 \( G \) must be isomorphic to \( \mathbb{Z}_6 \) or \( \mathbb{Z}_2 \times \mathbb{Z}_3 \). We do not need to include \( \mathbb{Z}_3 \times \mathbb{Z}_2 \) in the list since \( \mathbb{Z}_3 \times \mathbb{Z}_2 \) is isomorphic to \( \mathbb{Z}_6 \) by Lemma 16A.1(a); however, it turns out that the above list already includes a redundancy as \( \mathbb{Z}_2 \times \mathbb{Z}_3 \) is isomorphic to \( \mathbb{Z}_6 \).

Since operation in both \( \mathbb{Z}_2 \) and \( \mathbb{Z}_3 \) is denoted by +, we will use additive notation in \( \mathbb{Z}_2 \times \mathbb{Z}_3 \) as well (this is a standard convention); in particular, for an element \( g \in \mathbb{Z}_2 \times \mathbb{Z}_3 \) and \( l \in \mathbb{Z} \) we will write \( lg \) instead of \( g^l \).

By Theorem 15.2, to prove that \( \mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6 \), it suffices to prove that \( \mathbb{Z}_2 \times \mathbb{Z}_3 \) is cyclic. We claim that \( g = ([1],[1]) \) is a generator of \( \mathbb{Z}_2 \times \mathbb{Z}_3 \).

Indeed, for any \( l \in \mathbb{Z} \) we have

\[
lg = g + \ldots + g = ([1] + \ldots + [1], [1] + \ldots + [1]) = ([l],[l]),
\]

and \( ([l],[l]) \) is equal to \( ([0],[0]) \) if and only if \( l \) is both a multiple of 2 and a multiple of 3, that is, \( l \) is a multiple of 6. Thus, the smallest positive \( l \) such that \( lg = ([0],[0]) \) is \( l = 6 \), so \( o(g) = 6 = |\mathbb{Z}_2 \times \mathbb{Z}_3| \), so \( g \) is indeed a generator.

The result of the last example can be generalized as follows.

**Theorem 16A.3.** Let \( m, n \geq 2 \) be integers. Then \( \mathbb{Z}_n \times \mathbb{Z}_m \) is cyclic if and only if \( n \) and \( m \) are coprime. More generally, given any integers \( n_1, \ldots, n_k \) with \( n_i \geq 2 \), the group \( \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k} \) is cyclic if and only if \( n_1, \ldots, n_k \) are pairwise coprime.

The proof of this theorem is left as an exercise in Homework#8.

The following result is a direct consequence of Theorem 16A.3 and Theorem 15.2:

**Corollary 16A.4.** Let \( n \geq 2 \) be an integer, and write \( n = p_1^{a_1} \ldots p_k^{a_k} \) where \( p_1, \ldots, p_k \) are distinct primes. Then

\[
\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{a_1}} \times \ldots \times \mathbb{Z}_{p_k^{a_k}}.
\]
We can now state a stronger form of the classification theorem.

**Theorem 16A.5** (Fundamental Theorem of Finite Abelian Groups, prime factors form). Let $G$ be a finite abelian group with $|G| \geq 2$. Then there exist primes $p_1, \ldots, p_k$ (NOT necessarily distinct) and $a_1, \ldots, a_k \in \mathbb{N}$ such that

$$G \cong \mathbb{Z}_{p_1^{a_1}} \times \ldots \times \mathbb{Z}_{p_k^{a_k}}.$$

Moreover, the sequence of prime powers $p_1^{a_1}, \ldots, p_k^{a_k}$ appearing in the above factorization is uniquely determined by $G$ up to permutation.

The first (existence) part of Theorem 16A.5 is a consequence of Corollary 16A.4, Theorem 16A.2 and Lemma 16A.1. The moreover (uniqueness) part requires quite a bit of additional work which we will not discuss.

Theorem 16A.5 can be used to classify all finite abelian groups of any given order up to isomorphism. By **classifying up to isomorphism** we mean that given any $n \in \mathbb{N}$, we can write down a finite list of abelian groups of order $n$ such that any two groups in the list are not isomorphic to each other and any abelian group of order $n$ is isomorphic to some group on the list.

**Example 3.** Classify all abelian groups of order $48$.

By Theorem 16A.5 the classification problem reduces to finding all ways to write $48$ as a product of prime powers (where each prime power is assumed to be greater than $1$ and the order in which prime powers appear does not matter). We have $48 = 2^4 \cdot 3^1$. There is no way to split $3^1$, but $2^4$ can be written as a product of powers of $2$ in five different ways: $2^4 = 16$, $2^3 \cdot 2 = 8 \cdot 2$, $2^2 \cdot 2^2 = 4 \cdot 4$, $2^2 \cdot 2 \cdot 2 = 4 \cdot 2 \cdot 2$, and $2 \cdot 2 \cdot 2 \cdot 2$. The corresponding factorizations of $48$ are $16 \cdot 3$, $8 \cdot 2 \cdot 3$, $4 \cdot 4 \cdot 3$, $4 \cdot 2 \cdot 2 \cdot 3$ and $2 \cdot 2 \cdot 2 \cdot 2 \cdot 3$.

Thus, there are five abelian groups of order $48$ up to isomorphism, namely $\mathbb{Z}_{16} \times \mathbb{Z}_3$, $\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_3$, $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

If we analyze where the number $5$ came from in the above computation, we will see that it was completely determined by the exponents in the prime factorization of $48$ (namely, $4$ and $1$) and not by the primes themselves. In general, the number of pairwise non-isomorphic abelian groups of order $n$ can be expressed using the partition function.

**Definition.** Let $n \in \mathbb{N}$. A partition of $n$ is a way to write $n$ as a sum of positive integers where the order of summands does not matter. The number of distinct partitions of $n$ is denoted by $p(n)$, and the function $p$ is called the **partition function**.
For instance, \( p(1) = 1 \) (there is no way to split 1), \( p(2) = 2 \) (partitions of 2 are 2 itself and 1 + 1), \( p(3) = 3 \) (partitions of 3 are 3, 2 + 1 and 1 + 1 + 1) and \( p(4) = 5 \) (partitions of 4 are 4, 3 + 1, 2 + 2, 2 + 1 + 1 and 1 + 1 + 1 + 1). Based on this pattern, one may guess that the sequence \( p(2), p(3), p(4), \ldots \) is simply the sequence of all primes; however, this analogy only lasts up to \( p(6) = 11 \); the next value \( p(7) \) is 15, not 13.

**Theorem 16A.6.** Let \( n \geq 2 \) be an integer, and write \( n = p_1^{a_1} \ldots p_k^{a_k} \) where \( p_1, \ldots, p_k \) are distinct primes. Then the number of abelian groups of order \( n \) (up to isomorphism) is equal to \( \prod_{i=1}^{k} p(a_i) = p(a_1) \ldots p(a_k) \) where \( p \) is the partition function.

For instance, if \( n = 48 = 2^4 \cdot 3^1 \), we have \( k = 2, a_1 = 4 \) and \( a_2 = 1 \), so the number of groups of order 48 (up to isomorphism) is \( p(4)p(1) = 5 \cdot 1 = 5 \), which is consistent with the result of Example 3.

**Proof.** If we want to count the number of ways to write \( n = p_1^{a_1} \ldots p_k^{a_k} \) as a product of prime powers, we need to count the number of ways to split each of the powers \( p_i^{a_i} \) and then take the product of the obtained numbers. Writing \( p_i^{a_i} \) as a product of prime powers is equivalent to writing \( a_i \) as a sum of positive integers. Thus, the number of ways to write \( p_i^{a_i} \) as a product of prime powers is \( p(a_i) \), and the result follows. \( \square \)