Section II.11. Direct Products and Finitely Generated Abelian Groups

Note. In the previous section, we took given groups and explored the existence of subgroups. In this section, we introduce a process to build new (bigger) groups from known groups. This process will allow us to classify all finite abelian groups.

Definition 11.1. The Cartesian product of sets $S_1, S_2, \ldots, S_n$ of the set of all ordered $n$-tuples $(a_1, a_2, \ldots, a_n)$ where $a_i \in S_i$ for $i = 1, 2, \ldots, n$. This is denoted

$$\prod_{i=1}^{n} S_i = S_1 \times S_2 \times \cdots \times S_n.$$ 

Theorem 11.2. Let $G_1, G_2, \ldots, G_n$ be (multiplicative) groups. For $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in \prod G_i$, define the (multiplicative) binary operation

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n).$$

The $\prod G_i$ is a group under this binary operation, called the direct product of the groups $G_i$. 

II.11 Direct Products, Finitely Generated Abelian Groups

Note. If each $G_i$ is an additive group, then we may refer to $\prod G_i$ as the direct sum of the groups $G_i$ and denote it as

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n.$$  

However, this is simply a matter of notation—the concepts are always the same regardless of whether we use additive or multiplicative notation.

Note. Of course, if $|G_i| = r_i$ then $\left| \prod_{i=1}^{n} G_i \right| = r_1 r_2 \cdots r_n$.

Exercise 11.2. List the elements of $\mathbb{Z}_3 \times \mathbb{Z}_4$. Is this group cyclic?

Solution. Well, $\mathbb{Z}_3 \times \mathbb{Z}_4 = \{(a, b) \mid a \in \mathbb{Z}_3, b \in \mathbb{Z}_4\}$, so

$$\mathbb{Z}_3 \times \mathbb{Z}_4 = \{(0,0), (0,1), (0,2), (0,3), (1,0), (1,1), (1,2), (1,3), (2,0), (2,1), (2,2), (2,3)\}.$$  

Since 1 is a generator of both $\mathbb{Z}_3$ and $\mathbb{Z}_4$, let’s consider powers of $(1,1) \in \mathbb{Z}_3 \times \mathbb{Z}_4$:

$$\{n(1,1) \mid n \in \mathbb{Z}\} = \{(0,0), (1,1), (2,2), (0,3), (1,0), (2,1), (0,2), (1,3), (2,0), (0,1), (1,2), (2,3)\} = \mathbb{Z}_3 \times \mathbb{Z}_4.$$  

So $(1,1)$ is a generator of $\mathbb{Z}_3 \times \mathbb{Z}_4$ and it is cyclic.

Note. So we see that $\mathbb{Z}_3 \times \mathbb{Z}_4$ is a cyclic group of order 12. Now, $\mathbb{Z}_{12}$ is also a cyclic group of order 12. By Theorem 6.10, there is (up to isomorphism) only one cyclic group of order 12. So $\mathbb{Z}_3 \times \mathbb{Z}_4 \cong \mathbb{Z}_{12}$. 

Note. The trick of generating $\mathbb{Z}_3 \times \mathbb{Z}_4$ with element $(1, 1)$ will not work for just any product of groups. For example, $(1, 1)$ is not a generator of $\mathbb{Z}_2 \times \mathbb{Z}_2$: 

$$\{n(1, 1) \mid n \in \mathbb{Z}\} = \{(0, 0), (1, 1)\} \neq \mathbb{Z}_2 \times \mathbb{Z}_2.$$ 

Definition. For $r_1, r_2, \ldots, r_n \in \mathbb{N}$, the smallest element of $\mathbb{N}$ that is a multiple of each $r_i$ for $i = 1, 2, \ldots, n$, is the least common multiple of the $r_i$, denoted $\text{lcm}(r_1, r_2, \ldots, r_n)$.

**Theorem 11.5.** The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and isomorphic to $\mathbb{Z}_{mn}$ if and only if $m$ and $n$ are relatively prime (i.e., $\gcd(m, n) = 1$).

Note. Theorem 11.5 can be generalized to a direct product of several cyclic groups:

**Corollary 11.6.** The group $\prod_{i=1}^{n} \mathbb{Z}_{m_i}$ is cyclic and isomorphic to $\mathbb{Z}_{m_1m_2\cdots m_n}$ if and only if $m_i$ and $m_j$ are relatively prime for $i \neq j$. That is, $\gcd(m_i, m_j) = 1$ if $i \neq j$.

Note. If the $m_i$’s of Corollary 11.6 are powers of different primes, then $\gcd(m_i, m_j) = 1$ and so we can conclude:

**Corollary.** Let $p_1, p_2, \ldots, p_r$ be different prime numbers and let $n_1, n_2, \ldots n_r \in \mathbb{N}$. Define $m_k = (p_k)^{n_k}$. Then $\mathbb{Z}_{m_1m_2\cdots m_r} = \mathbb{Z}_{(p_1)^{n_1}(p_2)^{n_2}(p_r)^{n_r}}$ is isomorphic to

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r} = \mathbb{Z}_{(p_1)^{n_1}} \times \mathbb{Z}_{(p_2)^{n_2}} \times \cdots \times \mathbb{Z}_{(p_r)^{n_r}}.$$
Example. This corollary allows us to conclude the following: $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$, $\mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4$, $\mathbb{Z}_{30} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$, $\mathbb{Z}_{210} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$, etc.

**Theorem 11.9.** Let $(a_1, a_2, \ldots, a_n) \in \mathbb{P} G_i$. If $a_i$ is of finite order $r_i$ in $G_i$, then the order of $(a_1, a_2, \ldots, a_n)$ in $\mathbb{P} G_i$ is the least common multiple of the $r_i$, $\text{lcm}(r_1, r_2, \ldots, r_n)$.

**Exercise 11.6.** Find the order of $(3, 10, 9)$ in $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{15}$.

**Solution.** To use Theorem 11.9, we need to find the orders of the elements in their respective cyclic groups. By Theorem 6.14, the order of 3 in $\mathbb{Z}_4$ is $4/\gcd(3, 4) = 4/1 = 4$. The order of 10 in $\mathbb{Z}_{12}$ is $12/\gcd(10, 12) = 12/2 = 6$. The order of 9 in $\mathbb{Z}_{15}$ is $15/\gcd(9, 15) = 15/3 = 5$. So by Theorem 11.9, $(3, 10, 9)$ is of order $\text{lcm}(4, 6, 5) = 60$.

Note. The following is a very big deal! Part of the goal of algebra is to classify all groups. Cayley’s Theorem (Theorem 8.16) tells us that every group is a group of permutations. However, this does not tell us much about what the groups are. The following result, on the other hand, gives the exact structure of each finitely generated abelian group.

Every finitely generated abelian group $G$ is isomorphic to a direct product of cyclic groups in the form

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \cdots \times \mathbb{Z}$$

where the $p_i$ are primes, not necessarily distinct, and the $r_i$ are positive integers. The direct product is unique except for possible rearrangement of the factors; that is, the number of factors of $\mathbb{Z}$ is unique (called the Betti number of $G$) and the prime powers $(p_i)^{r_i}$ are unique.

Note. The proof of this is complicated and given in Section VII.38.

Note. As a corollary, we can observe that for a finite abelian group the Betti number is 0 and the structure is given by a direct product of cyclic groups of orders of certain powers of primes.
Exercise 11.24. Find all abelian groups (up to isomorphism) of order 720.

Solution. First, we need to factor 720: $720 = 2^4 \cdot 3^2 \cdot 5$. For the factor $2^4$ we get the following groups (this is a list of non-isomorphic groups by Theorem 11.5):

- $\mathbb{Z}_{16}$
- $\mathbb{Z}_2 \times \mathbb{Z}_8$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
- $\mathbb{Z}_4 \times \mathbb{Z}_4$

The factor $3^2$ yields: $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$. Factor 5 yields: $\mathbb{Z}_5$. So we get a total of 10 possible groups of order 720:

- $\mathbb{Z}_{16} \times \mathbb{Z}_9 \times \mathbb{Z}_5$
- $\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
- $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

Definition 11.14. A group $G$ is decomposable if it is isomorphic to a direct product of two proper nontrivial subgroups. Otherwise $G$ is indecomposable.

Theorem 11.15. The finite indecomposable abelian groups are exactly the cyclic groups with order a power of a prime.

Note. Recall that Lagrange's Theorem implies that the order of a subgroup must divide the order of the group. The converse does not hold in general since $A_4$ (of order $4!/2 = 12$) has no subgroup of order 6 (this will be shown in Example 15.6 on page 146). The following result shows that the converse of Lagrange's Theorem does hold for abelian groups.
**Theorem 11.16.** If \( m \) divides the order of a finite abelian group \( G \), then \( G \) has a subgroup of order \( m \).

**Note.** Theorem 11.16 does not hold in general for nonabelian groups, but it does hold in the special case when \( m \) is prime. Namely, we have the following which is Theorem 36.3 from page 322:

**Cauchy’s Theorem.** Let \( p \) be prime. Let \( G \) be a finite group and suppose \( p \) divides \( |G| \). Then \( G \) has a subgroup of order \( p \).

The fact that Cauchy’s Theorem does not appear for another 200 pages implies that we have a good deal more information to learn before we can get deeper into this aspect of our exploration of group theory.

**Theorem 11.17.** If \( m \) is a square free integer (that is, no prime factor of \( m \) is of multiplicity greater than 1), then every abelian group of order \( m \) is cyclic.