11 Direct Products and Finitely Generated Abelian Groups

A review of the groups we have seen so far:

$$\begin{aligned}
\mathbb{Z}_n &= \text{cyclic group of addition modulo } n \\
S_n &= \text{symmetric group of permutations} \\
A_n \leq S_n &= \text{alternating group consisting of all even permutations of } n \text{ letters} \\
D_n &= \text{dihedral group of symmetries of the regular } n\text{-gon} \\
V &= \text{Klein-4 group} \\
U &= \text{complex numbers of magnitude 1 (on unit circle) under multiplication}
\end{aligned}$$

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

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

Theorem. *Let $G_1, G_2, \ldots, G_n$ be groups. For $(a_1, a_2, \ldots, a_n) \in \prod_{i=1}^{n} G_i$ and $(b_1, b_2, \ldots, b_n) \in \prod_{i=1}^{n} G_i$, define*

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n).$$

Then $\prod_{i=1}^{n} G_i$ is a group, the ***direct product of the groups*** G_i, *under this binary operation.*

Remark. *If the operation of each G_i is commutative, we define* ***direct sum of the groups*** G_i *with addition as the binary operation:*

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

and

$$\bigoplus_{i=1}^{n} G_i = G_1 \oplus G_2 \cdots \oplus G_n.$$

If each S_i has n_i elements, then how many elements would $\prod_{i=1}^{n} S_i$ have?

Example 1. *We have $\langle(1, 1)\rangle = \mathbb{Z}_3 \times \mathbb{Z}_2$:*

$$\begin{aligned}
1(1, 1) &= (1, 1) \\
2(1, 1) &= (1, 1) + (1, 1) = (2, 0) \\
3(1, 1) &= (2, 0) + (1, 1) = (0, 1) \\
4(1, 1) &= (0, 1) + (1, 1) = (1, 0) \\
5(1, 1) &= (1, 0) + (1, 1) = (2, 1) \\
6(1, 1) &= (2, 1) + (1, 1) = (0, 0)
\end{aligned}$$

Since there is only one cyclic group of a given order (up to isomorphism), we have $\mathbb{Z}_3 \oplus \mathbb{Z}_2 \cong \mathbb{Z}_6$.

Example 2. *The group $\mathbb{Z}_2 \times \mathbb{Z}_2$ is* not *cyclic, because the maximum order of every element is 2 and there is no element of order 4 to generate the entire group. Therefore $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V$.*

Theorem.

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \Longleftrightarrow \gcd(m, n) = 1.$$

Corollary.

$$\prod_{i=1}^{n} \mathbb{Z}_{m_i} \cong \mathbb{Z}_{m_1 m_2 \cdots m_n} \Longleftrightarrow \gcd(m_i, m_j) = 1, i \neq j$$

Example 3.

$$\mathbb{Z}_{120} \cong \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

Remark.

$$G_1 \times G_2 \cong G_2 \times G_1$$

Remark. *Let H be the set of all common multiples of positive integers $r_i, i = 1, 2, \ldots, n$. Then $H \leq \mathbb{Z}$ and hence H is cyclic.*

Definition. *Let $r_1, r_2, \ldots, r_n \in \mathbb{Z}^+$. Their **least common multiple** (denoted by lcm) is the positive generator of the cyclic group of all common multiples of the r_i, that is, the cyclic group of all integers divisible by each r_i for $i = 1, 2, \ldots, n$.*

Theorem. *Let $(a_1, a_2, \ldots, a_n) \in \prod_{i=1}^n G_i$. If a_i is of finite order r_i in G_i, then the order of $(a_1, a_2, \ldots, a_n)$ in $\prod_{i=1}^n G_i$ is equal to $\mathrm{lcm}(r_1, r_2, \ldots, r_n)$.*

Example 4. *Find the order of $(3, 6, 12, 16)$ in $\mathbb{Z}_4 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{20} \oplus \mathbb{Z}_{24}$.*

Remark. *Let*

$$\bar{G}_i = \{(e_1, e_2, \ldots, e_{i-1}, a_i, e_{i+1}, \ldots, e_n) \mid a_i \in G_i\},$$

that is, the set of all n-tuples with the identity elements in all places except the ith place. Then $\bar{G}_i \leq \prod_{i=1}^n G_i$. Furthermore, $\bar{G}_i \cong G_i$ because $(e_1, e_2, \ldots, e_{i-1}, a_i, e_{i+1}, \ldots, e_n)$ corresponds to a_i.

We say $\prod_{i=1}^n G_i$ is the internal direct product *of the subgroups $\bar{G}_i$ and the usual direct product is called the* external *direct product of the groups G_i. So, internal refers to subgroups and external to groups.*

11.0.1 The Structure of Finitely Generated Abelian Groups

Theorem (Fundamental Theorem of Finitely Generated Abelian Groups)**.** *Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups in the form*

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

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 (**Betti number** of G) of factors $\mathbb{Z}$ is unique and the prime powers $(p_i)^{r_i}$ are unique.*

Example 5. *Find all abelian groups, up to isomorphism, of order*

a) 16

b) 720

c) 10^4

11.0.2 Applications

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

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

Theorem. *If m divides the order of a finite abelian group G, then G has a subgroup of order m.*

Theorem. *If m is a square free integer, that is, m is not divisible by the square of any prime, then every abelian group of order m is cyclic.*