Definition 8.1

The *direct product* of groups $G_1, \dots, G_n$ is a group $G_1 \times G_2 \times \dots \times G_n$ defined as follows:

- Elements: n-tuples $(g_1, g_2, \dots, g_n)$ where $g_i \in G_i$.
- Group operation:

$$(g_1, g_2, \dots, g_n) \cdot (h_1, h_2, \dots, h_n) = (g_1 h_1, g_2 h_2, \dots, g_n h_n)$$

- The identity element: $(e_1, e_2, \dots, e_n)$ where e_i is the identity element in G_i.
- Inverses: $(g_1, g_2, \dots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \dots, g_n^{-1})$.

Note. We have:

$$|G_1 \times G_2 \times \dots \times G_n| = |G_1| \cdot |G_2| \cdot \dots \cdot |G_n|$$

Example. The groups $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ has 6 elements:

$$(0,0),\ (0,1),\ (0,2),\ (1,0),\ (1,1),\ (1,2)$$

The multiplication table in $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is as follows:

$\circ$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,0)$	$(0,0)$	$(0,1)$	$(0,1)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,1)$	$(0,1)$	$(0,2)$	$(0,0)$	$(1,1)$	$(1,2)$	$(1,0)$
$(0,2)$	$(0,2)$	$(0,0)$	$(0,1)$	$(1,2)$	$(1,0)$	$(1,1)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,2)$	$(0,0)$	$(0,1)$	$(0,2)$
$(1,1)$	$(1,1)$	$(1,2)$	$(1,0)$	$(0,1)$	$(0,2)$	$(0,0)$
$(1,2)$	$(1,2)$	$(1,0)$	$(1,1)$	$(0,2)$	$(0,0)$	$(0,1)$

Theorem 8.2

The group $G_1 \times \dots \times G_n$ is abelian of and only if each of the groups G_i is abelian.

Proof. If $G_1, \ldots, G_n$ are abelian groups, then

$$\begin{aligned}(g_1, \ldots, g_n) \cdot (h_1, \ldots, h_n) &= (g_1 h_1, \ldots, g_n h_n) \\ &= (h_1 g_1, \ldots, h_n g_n) = (h_1, \ldots, h_n) \cdot (g_1, \ldots, g_n)\end{aligned}$$

Conversely, if $G_1 \times \ldots \times G_n$ is abelian then for any $g_i, h_i \in G_i$ we have

$$\begin{aligned}(g_1 h_1, \ldots, g_n h_n) &= (g_1, \ldots, g_n) \cdot (h_1, \ldots, h_n) \\ &= (h_1, \ldots, h_n) \cdot (g_1, \ldots, g_n) = (h_1 g_1, \ldots, h_n g_n)\end{aligned}$$

which gives $g_i h_i = h_i g_i$ for $i = 1, \ldots, n$. □

Recall:

- The *least common multiple* of integers $n_1, n_2, \ldots, n_k \geq 1$ is the smallest positive integer, denoted by $\mathrm{lcm}(n_1, \ldots, n_k)$, which is divisible by each of these numbers.
- If $m > 0$ is an integer divisible by $n_1, \ldots, n_k$ then m is divisible by $\mathrm{lcm}(n_1, \ldots, n_k)$.

Theorem 8.3

For $i = 1, \ldots, n$ let $a_i \in G_i$, and let $(a_1, \ldots, a_n) \in G_1 \times \ldots \times G_n$. Then

$$|(a_1, \ldots, a_n)| = \mathrm{lcm}(|a_1|, \ldots, |a_n|)$$

Example. Consider the element $(1, 1) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ since $1 \in Z_2$ is an element of order 2, and $1 \in \mathbb{Z}_3$ is an element of order 3, we obtain that $|(1, 1)| = \mathrm{lcm}(2, 3) = 6$.

Proof of Theorem 8.3. Let $|(a_1, \ldots, a_n)| = p$ and $\mathrm{lcm}(|a_1|, \ldots, |a_n|) = q$. We have

$$(a_1, \ldots, a_n)^q = (a_1^q, \ldots, a_n^q) = (e_1, \ldots, e_n)$$

The last equality comes from Theorem 6.3, since $|a_i|$ divides q for each i. Using Theorem 6.3 again we obtain that p divides q. On the other hand,

$$(e_1, \ldots, e_n) = (a_1, \ldots, a_n)^p = (a_1^p, \ldots, a_n^p)$$

which gives $e_i = a_i^p$ for each i. Using Theorem 6.3 one more time, we get that $|a_i|$ divides p, and so $q = \mathrm{lcm}(|a_1|, \ldots, |a_n|)$ divides p. As a consequence $p = q$. □