SECTION 11: DIRECT PRODUCTS

So far, we’ve talked about cyclic groups, symmetric groups, and dihedral groups. Today, we will introduce a notion called direct product that allows us to build new groups!

**Definition 0.1.** Let $A$ and $B$ be sets. The **Cartesian product** of $A$ and $B$ is denoted $A \times B$ and is the set of all pairs $(a, b)$ such that $a \in A$ and $b \in B$:

$$A \times B = \{(a,b) \mid a \in A, b \in B\}.$$  

We can also form the Cartesian product of $n$ sets $A_1, A_2, \ldots, A_n$:

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i\}.$$  

For simplicity, this is sometimes denoted by

$$A_1 \times A_2 \times \cdots \times A_n = \prod_{i=1}^{n} A_i.$$  

**Example 0.2.** You have been secretly familiar with Cartesian products for a long time as you’ve used Cartesian coordinates: we write $\mathbb{R}^2$ for the plane whose points are $(x, y)$, where $x$ and $y$ are real numbers, but this is just saying

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}.$$  

**Example 0.3.** List all elements of $\mathbb{Z}_2 \times \mathbb{Z}_3$. How many elements are in $\mathbb{Z}_2 \times \mathbb{Z}_3$?

We know $\mathbb{Z}_2 = \{0, 1\}$ and $\mathbb{Z}_3 = \{0, 1, 2\}$, so the elements of $\mathbb{Z}_2 \times \mathbb{Z}_3$ are:

$(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)$.

**Remark 0.4.** If $|A| = n$ and $|B| = m$, then $|A \times B| = nm$: there are $n$ choices for the first element and $m$ for the second.

What does this have to do with groups?

**Definition 0.5.** Let $G_1$ and $G_2$ be groups. For any $(g_1, g_2), (h_1, h_2) \in G_1 \times G_2$, define a binary operation on $G_1 \times G_2$ by $(g_1, g_2) \times (h_1, h_2) = (g_1 h_1, g_2 h_2)$. The **direct product** of $G_1$ and $G_2$ is the group $G_1 \times G_2$ with this binary operation.

Similarly, if we have more than two groups, we can define a binary operation on $G_1 \times G_2 \times \cdots \times G_n$ by $(g_1, g_2, \ldots, g_n) \times (h_1, h_2, \ldots, h_n) = (g_1 h_1, g_2 h_2, \ldots, g_n h_n)$.

In $G_1 \times G_2$ (or $G_1 \times G_2 \times \cdots \times G_n$), the identity is $(e_1, e_2)$ (or $(e_1, e_2, \ldots, e_n)$), where $e_i$ is the identity element of $G_i$. For any element $(g_1, g_2) \in G_1 \times G_2$ (or $(g_1, g_2, \ldots, g_n) \in G_1 \times G_2 \times \cdots \times G_n$), the inverse is $(g_1^{-1}, g_2^{-1})$ (or $(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$).

If $G_1$ and $G_2$ are abelian groups, by definition of the binary operation, $G_1 \times G_2$ is also abelian. Some textbooks use the notation $G_1 \oplus G_2$ instead of $G_1 \times G_2$ in this case, but ours uses $\times$, so we’ll stick with that.

Let’s practice!

**Example 0.6.** What is the identity element in $\mathbb{Z}_2 \times \mathbb{Z}_3$? What is the inverse of $(1, 2)$? What is the order of $(1, 1)$?
The identity element is \((0,0)\); the inverse of \((1,2)\) is \((1,1)\) (because the inverse of \(1 \in \mathbb{Z}_2\) is 1 and the inverse of \(2 \in \mathbb{Z}_3\) is 1). To find the order of \((1,1)\), we need to figure out how many times we must add \((1,1)\) to itself to get back to the identity. Let’s do that:

\[
\begin{align*}
(1,1) &= (1,1) \\
(1,1) + (1,1) &= (0,2) \\
(1,1) + (1,1) + (1,1) &= (1,0) \\
(1,1) + (1,1) + (1,1) + (1,1) &= (0,1) \\
(1,1) + (1,1) + (1,1) + (1,1) + (1,1) &= (1,2) \\
(1,1) + (1,1) + (1,1) + (1,1) + (1,1) + (1,1) &= (0,0)
\end{align*}
\]

We see that \(n(1,1) = (0,0)\) when \(n = 6\) (and no smaller positive integer), so the order of \((1,1)\) is 6.

This proves something! We know that a group of size \(n\) is cyclic if and only if there exists an element of order \(n\). We saw that \(\mathbb{Z}_2 \times \mathbb{Z}_3\) had size 6, and we just found an element of order 6, and see that \(\mathbb{Z}_2 \times \mathbb{Z}_4 = \langle (1,1) \rangle\) so \(\mathbb{Z}_2 \times \mathbb{Z}_4\) is cyclic. It is cyclic of order 6, so \(\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6\).

**Example 0.7.** Write out the elements of \(\mathbb{Z}_2 \times \mathbb{Z}_4\). Is this group cyclic? (Hint: try to find the maximal order of any element.)

The elements are \((0,0), (0,1), (0,2), (0,3), (1,0), (1,1), (1,2), (1,3)\). By direct computation, we could check that each element has order at most 4, but let’s do it more generally. If \((r,s)\) is any element of \(\mathbb{Z}_2 \times \mathbb{Z}_4\), then \(4(r,s) = (r,s) + (r,s) + (r,s) + (r,s) = (4r, 4s) = (0,0)\), because \(4 = 0 \mod 2\) and \(4 = 0 \mod 4\). So, for any element in \(\mathbb{Z}_2 \times \mathbb{Z}_4\), the order is at most 4. Therefore, \(\mathbb{Z}_2 \times \mathbb{Z}_4\) is not cyclic, as it has no element of order 8.

This is an example of a more general phenomenon.

**Theorem 0.8.** The group \(\mathbb{Z}_m \times \mathbb{Z}_n\) is cyclic and isomorphic to \(\mathbb{Z}_{mn}\) if and only if \(\gcd(m, n) = 1\).

**Proof.** Suppose \(\gcd(m, n) = 1\) and consider the subgroup \(\langle (1,1) \rangle\). The order is the smallest positive multiple \(a\) of \((1,1)\) such that \(a(1,1) = (0,0)\). But, \(a(1,1) = (a, a)\), and if \((a, a) = (0,0)\), then \(a = 0 \mod m\) and \(a = 0 \mod n\). In other words, \(a\) must be divisible by both \(m\) and \(n\). Because \(m\) and \(n\) are relatively prime, this implies that \(a\) is divisible by \(mn\). Since we are looking for the smallest possible \(a\) such that \(a(1,1) = (0,0)\), this implies that \(a = mn\). So, the order of \(\langle (1,1) \rangle = mn = |\mathbb{Z}_m \times \mathbb{Z}_n|\), so \(\mathbb{Z}_m \times \mathbb{Z}_n\) is cyclic and of size \(mn\), so must be isomorphic to \(\mathbb{Z}_{mn}\).

Now suppose \(\gcd(m, n) = d > 1\). Then, \(a = mn/d\) is an integer that is divisible by both \(m\) and \(n\), so for any element \((r,s) \in \mathbb{Z}_m \times \mathbb{Z}_n\), \(a(r,s) = (ar, as) = (0,0)\), so the order of \((r,s)\) is at most \(a\). Because \(d > 1\), \(a < mn\), so the order of every element is strictly less than \(mn\), so \(\mathbb{Z}_m \times \mathbb{Z}_n\) is not cyclic. \(\square\)

Now, we try with more groups.

**Example 0.9.** Is \(\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4\) cyclic?

This group has \(2 \times 3 \times 4 = 24\) elements, but 12 is divisible by 2, 3, and 4, so for any element \((r,s,t) \in \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4\), \(12(r,s,t) = (0,0,0)\), so each element has order at most 12, hence this group is not cyclic.
You can prove the following theorem in the same way as the previous one.

**Theorem 0.10.** The group $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$ is cyclic and isomorphic to $\mathbb{Z}_{m_1 m_2 \cdots m_n}$ if and only if $\gcd(m_i, m_j) = 1$ for every pair $(m_i, m_j)$.

We can also say something about the order of elements in (finite) direct product groups.

**Theorem 0.11.** Let $(a_1, a_2, \ldots, a_n) \in G_1 \times G_2 \times \cdots \times G_n$, where each $G_i$ is a finite group. Let $r_i$ be the order of $a_i$ in $G_i$. Then, the order of $(a_1, a_2, \ldots, a_n)$ is equal to $\text{lcm}(r_1, r_2, \ldots, r_n)$.

**Proof.** If $k = \text{lcm}(r_1, r_2, \ldots, r_n)$, then $k$ is the smallest positive integer that is divisible by each $r_i$. Because it is divisible by each $r_i$, $a_i^k = e_i$, so $(a_1, a_2, \ldots, a_n)^k = (e_1, e_2, \ldots, e_n)$. Because $k$ is the smallest integer with this property, the order of $(a_1, a_2, \ldots, a_n)$ must equal $k$. \qed

**Example 0.12.** Find the order of $(8, 4, 10)$ in $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$.

We compute that the order of $8 \in \mathbb{Z}_{12}$ is $3$; the order of $4$ in $\mathbb{Z}_{60}$ is $15$, and the order of $10$ in $\mathbb{Z}_{24}$ is $12$, so the order of $(8, 4, 10)$ is $\text{lcm}(4, 15, 12) = 60$. 

3