Direct Products

- The Cartesian product \( G \times H \) of groups \( G \) and \( H \) becomes a group under \textit{componentwise multiplication}: 
  \[(g_1, h_1) \cdot (g_2, h_2) = (g_1g_2, h_1h_2) \text{ for } (g_1, h_1), (g_2, h_2) \in G \times H. \] 
  \( G \times H \) is called the \textbf{direct product} of \( G \) and \( H \).

- If \( G \) and \( H \) are finite, \( |G \times H| = |G||H| \).

- The direct product of abelian groups is an abelian group.

- The order of \((1, 1) \in \mathbb{Z}_m \times \mathbb{Z}_n\) is \([m, n]\).

- \( \mathbb{Z}_m \times \mathbb{Z}_n \approx \mathbb{Z}_{mn} \) — i.e., \( \mathbb{Z}_m \times \mathbb{Z}_n \) is cyclic of order \( mn \) — if and only if \( (m, n) = 1 \).

**Definition.** Let \( G \) and \( H \) be groups. The \textbf{direct product} \( G \times H \) of \( G \) and \( H \) is the set of all ordered pairs \( \{(g, h) \mid g \in G, h \in H\} \) with the operation 

\[(g_1, h_1) \cdot (g_2, h_2) = (g_1g_2, h_1h_2).\]

**Remarks.**
1. In the definition, I’ve assumed that \( G \) and \( H \) are using multiplication notation. In general, the notation you use in \( G \times H \) depends on the notation in the factors. Examples:

<table>
<thead>
<tr>
<th>( G )</th>
<th>( H )</th>
<th>Product ( (G \times H) )</th>
<th>Identity ( (G \times H) )</th>
<th>Inverse ( (G \times H) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( g_1 \cdot g_2 )</td>
<td>( h_1 \cdot h_2 )</td>
<td>((g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2))</td>
<td>( (1, 1) )</td>
<td>((g, h)^{-1} = (g^{-1}, h^{-1}))</td>
</tr>
<tr>
<td>( g_1 + g_2 )</td>
<td>( h_1 + h_2 )</td>
<td>((g_1, h_1) + (g_2, h_2) = (g_1 + g_2, h_1 + h_2))</td>
<td>( (0, 0) )</td>
<td>(-(g, h) = (-g, -h))</td>
</tr>
<tr>
<td>( g_1 \cdot g_2 )</td>
<td>( h_1 + h_2 )</td>
<td>((g_1, h_1)(g_2, h_2) = (g_1g_2, h_1 + h_2))</td>
<td>( (1, 0) )</td>
<td>((g, h)^{-1} = (g^{-1}, -h))</td>
</tr>
</tbody>
</table>

2. You can construct products of more than two groups in the same way. For example, if \( G_1, G_2, \) and \( G_3 \) are groups, then 

\[ G_1 \times G_2 \times G_3 = \{(x, y, z) \mid x \in G_1, y \in G_2, z \in G_3\}. \]

Just as with the two-factor product, you multiply elements componentwise. □

**Example. (A product of cyclic groups which is cyclic)** Since \( \mathbb{Z}_2 = \{0, 1\} \) and \( \mathbb{Z}_3 = \{0, 1, 2\}, \)

\[ \mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}. \]

If you take successive multiples of \((1, 1)\), you get 

\[(1, 1), (0, 2), (1, 0), (0, 1), (1, 2), (0, 0). \]

Since you can get the whole group by taking multiples of \((1, 1)\), it follows that \( \mathbb{Z}_2 \times \mathbb{Z}_3 \) is actually cyclic of order 6 — the same as \( \mathbb{Z}_6 \). □

**Example. (A product of cyclic groups which is not cyclic)** Since \( \mathbb{Z}_2 = \{0, 1\}, \)

\[ \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (1, 0), (0, 1), (1, 1)\}. \]
Here’s the operation table:

<table>
<thead>
<tr>
<th></th>
<th>(0, 0)</th>
<th>(1, 0)</th>
<th>(0, 1)</th>
<th>(1, 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0, 0)</td>
<td>(0, 0)</td>
<td>(1, 0)</td>
<td>(0, 1)</td>
<td>(1, 1)</td>
</tr>
<tr>
<td>(1, 0)</td>
<td>(1, 0)</td>
<td>(0, 0)</td>
<td>(1, 1)</td>
<td>(0, 1)</td>
</tr>
<tr>
<td>(0, 1)</td>
<td>(0, 1)</td>
<td>(1, 1)</td>
<td>(0, 0)</td>
<td>(1, 0)</td>
</tr>
<tr>
<td>(1, 1)</td>
<td>(1, 1)</td>
<td>(0, 1)</td>
<td>(1, 0)</td>
<td>(0, 0)</td>
</tr>
</tbody>
</table>

Note that this is not the same group as \( \mathbb{Z}_4 \). Both groups have 4 elements, but \( \mathbb{Z}_4 \) is cyclic of order 4.

In \( \mathbb{Z}_2 \times \mathbb{Z}_2 \), all the elements have order 2, so no element generates the group.

\( \mathbb{Z}_2 \times \mathbb{Z}_2 \) is the same as the **Klein 4-group** \( V \), which has the following operation table:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>1</td>
<td>c</td>
<td>b</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>1</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>b</td>
<td>a</td>
<td>1</td>
</tr>
</tbody>
</table>

Compare the diagonal entries of the two tables, for instance. □

---

**Example.** *(The order of a product)* If \( G \) and \( H \) are finite, then \(|G \times H| = |G||H|\). For example, \(|\mathbb{Z}_5 \times \mathbb{Z}_6| = 30\). □

---

**Lemma.** The product of abelian groups is abelian: If \( G \) and \( H \) are abelian, so is \( G \times H \).

**Proof.** Suppose \( G \) and \( H \) are abelian. Let \((g, h), (g', h') \in G \times H\), where \( g, g' \in G \) and \( h, h' \in H \). I have

\[
(g, h)(g', h') = (gg', hh') \quad \text{(Definition of multiplication in a product)} \\
= (g'g, h'h) \quad \text{ (G and H are abelian)} \\
= (g', h')(g, h) \quad \text{(Definition of multiplication in a product)}
\]

This proves that \( G \times H \) is abelian. □

On the other hand, if either \( G \) or \( H \) is not abelian, then \( G \times H \) is not abelian. Suppose, for instance, that \( G \) is not abelian. This means that there are elements \( g_1, g_2 \in G \) such that

\[
g_1g_2 \neq g_2g_1.
\]

Then

\[
(g_1, 1)(g_2, 1) = (g_1g_2, 1), \quad \text{while} \quad (g_2, 1)(g_1, 1) = (g_2g_1, 1).
\]

Since \((g_1g_2, 1) \neq (g_2g_1, 1)\), it follows that \((g_1, 1)(g_2, 1) \neq (g_2, 1)(g_1, 1)\), so \( G \times H \) is not abelian.

A similar argument works if \( H \) is not abelian. □

---

**Example.** *(A product of an abelian and a nonabelian group)* The next two tables comprise the multiplication table for \( \mathbb{Z}_2 \times D_3 \). (Recall that \( D_3 \) is the group of symmetries of an equilateral triangle.) The number of elements is

\[
|\mathbb{Z}_2 \times D_3| = |\mathbb{Z}_2| \cdot |D_3| = 2 \cdot 6 = 12.
\]
When you multiply two pairs, you add.

Example. (Using products to construct groups) You can use products to construct 3 different abelian groups of order 8.
The groups $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, and $\mathbb{Z}_8$ are abelian, since each is a product of abelian groups. $\mathbb{Z}_8$ is cyclic of order 8, $\mathbb{Z}_4 \times \mathbb{Z}_2$ has an element of order 4 but is not cyclic, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has only elements of order 2. It follows that these groups are distinct.

The group $D_4$ of symmetries of the square is a nonabelian group of order 8.

The fifth (and last) group of order 8 is the group $Q$ of the quaternions.

$D_4$ or $Q$ are not that same as $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, or $\mathbb{Z}_8$, since $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, and $\mathbb{Z}_8$ are abelian while $D_4$ or $Q$ are not.

Finally, $D_4$ is not the same as $Q$. $D_4$ has 5 elements of order 2: The four reflections and rotation through 180°. $Q$ has one element of order 2, namely $-1$.

I’ve shown that these five groups of order 8 are distinct; it takes considerably more work to show that these are the only groups of order 8.

**Definition.** Let $m$ and $n$ be positive integers. The least common multiple $[m, n]$ of $m$ and $n$ is the smallest positive integer divisible by $m$ and $n$.

**Remark.** Since $mn$ is divisible by $m$ and $n$, the set of positive multiples of $m$ and $n$ is nonempty. Hence, it has a smallest element, by well-ordering. It follows that the least common multiple of two positive integers is always defined. For example, $[18, 30] = 90$.

**Lemma.** If $s$ is a common multiple of $m$ and $n$, then $[m, n] | s$.

**Proof.** By the Division Algorithm,

$$s = q \cdot [m, n] + r, \quad \text{where} \quad 0 \leq r < [m, n].$$

Thus, $r = s - q \cdot [m, n]$. Since $m | s$ and $m | [m, n]$, I have $m \mid r$. Since $n \mid s$ and $n \mid [m, n]$, I have $n \mid r$. Therefore, $r$ is a common multiple of $m$ and $n$. Since it’s also less than the least common multiple $[m, n]$, it can’t be positive. Therefore, $r = 0$, and $s = q \cdot [m, n]$, i.e. $[m, n] | s$. □

**Remark.** The lemma shows that the least common multiple is not just “least” in terms of size. It’s also “least” in the sense that it divides every other common multiple.

**Theorem.** Let $m$ and $n$ be positive integers. Then $mn = (m, n)[m, n]$.

**Proof.** I’ll prove that each side is greater than or equal to the other side.

Note that $\frac{m}{(m, n)}$ and $\frac{n}{(m, n)}$ are integers. Thus,

$$\frac{mn}{(m, n)} = m \cdot \frac{n}{(m, n)} = \frac{m}{(m, n)} \cdot n$$

is a multiple of $m$ and a multiple of $n$. Therefore, it’s a common multiple of $m$ and $n$, so it must be greater than or equal to the least common multiple. Hence,

$$\frac{mn}{(m, n)} \geq [m, n], \quad \text{and} \quad mn \geq (m, n)[m, n].$$

Next, $[m, n]$ is a multiple of $n$, so $[m, n] = sn$ for some $s$. Then

$$\frac{mn}{[m, n]} = \frac{mn}{sn} = \frac{m}{s} \mid m.$$  

(Why is $\frac{mn}{[m, n]}$ an integer? Well, $mn$ is a common multiple of $m$ and $n$, so by the previous lemma $[m, n] \mid mn.$)
Similarly, \([m, n]\) is a multiple of \(m\), so \([m, n] = tm\) for some \(t\). Then
\[
\frac{mn}{[m, n]} = \frac{mn}{tm} = \frac{n}{t} | n.
\]

In other words, \(\frac{mn}{[m, n]}\) is a common divisor of \(m\) and \(n\). Therefore, it must be less than the greatest common divisor:
\[
\frac{mn}{[m, n]} \leq (m, n), \quad \text{and} \quad mn \leq (m, n)[m, n].
\]

The two inequalities I’ve proved show that \(mn = (m, n)[m, n]\). \(\square\)

**Example. (The order of an element in a product)** \((54, 72) = 18, \ [54, 72] = 216, \) and
\[(54, 72)(54, 72) = 18 \cdot 216 = 3888 = 54 \cdot 72. \square\]

**Proposition.** The element \((1, 1)\) has order \([m, n]\) in \(\mathbb{Z}_m \times \mathbb{Z}_n\).

**Proof.**
\([m, n](1, 1) = ([m, n], [m, n])\).

The first component is 0, since it’s divisible by \(m\); the second component is 0, since it’s divisible by \(n\). Hence, \([m, n](1, 1) = (0, 0)\).

Next, I must show that \([m, n]\) is the smallest positive multiple of \((1, 1)\) which equals the identity. Suppose \(k(1, 1) = (0, 0)\), so \((k, k) = (0, 0)\). Consider the first components. \(k = 0\) in \(\mathbb{Z}_m\) means that \(m | k\); likewise, the second components show that \(n | k\). Since \(k\) is a common multiple of \(m\) and \(n\), it must be greater than or equal to the least common multiple \([m, n]\): that is, \(k \geq [m, n]\). This proves that \([m, n]\) is the order of \((1, 1)\). \(\square\)

**Example. (The order of \((1, 1)\))** In \(\mathbb{Z}_4 \times \mathbb{Z}_6\), the element \((1, 1)\) has order \([4, 6] = 12\).

On the other hand, the element \((1, 1) \in \mathbb{Z}_5 \times \mathbb{Z}_6\) has order 30. Since \(\mathbb{Z}_5 \times \mathbb{Z}_6\) has order 30, the group is cyclic; in fact, \(\mathbb{Z}_5 \times \mathbb{Z}_6 \approx \mathbb{Z}_{30}\). \(\square\)

**Remark.** More generally, consider \((x_1, \ldots, x_n) \in G_1 \times \ldots \times G_n\), and suppose \(x_i\) has order \(r_i\) in \(G_i\). (The \(G_i’s\) need not be cyclic.) Then \((x_1, \ldots, x_n)\) has order \([r_1, \ldots, r_n]\). \(\square\)

**Corollary.** \(\mathbb{Z}_m \times \mathbb{Z}_n\) is cyclic of order \(mn\) if and only if \((m, n) = 1\).

**Proof.** If \((m, n) = 1\), then \([m, n] = mn\). Thus, the order of \((1, 1)\) is \([m, n] = mn\). But \(\mathbb{Z}_m \times \mathbb{Z}_n\) has order \(mn\), so \((1, 1)\) generates the group. Hence, \(\mathbb{Z}_m \times \mathbb{Z}_n\) is cyclic.

Suppose on the other hand that \((m, n) \neq 1\). Since \((m, n)[m, n] = mn\), it follows that \([m, n] \neq mn\). Since \(mn\) is a common multiple of \(m\) and \(n\) and since \([m, n]\) is the least common multiple, it follows that \([m, n] < mn\).

Now consider an element \((a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n\). Let \(p\) be the order of \(a\) in \(\mathbb{Z}_m\) and let \(q\) be the order of \(b\) in \(\mathbb{Z}_n\).

Since \(p | m | [m, n]\), I may write \(pj = [m, n]\) for some \(j\). Since \(q | n | [m, n]\), I may write \(qk = [m, n]\) for some \(k\). Then
\[
[m, n](a, b) = ([m, n]a, [m, n]b) = (j(pa), k(qb)) = (j \cdot 0, k \cdot 0) = (0, 0).
\]

Hence, the order of \((a, b)\) is less than or equal to \([m, n]\). But \([m, n] < mn\), so the order of \((a, b)\) is less than (and not equal to) \(mn\).
Since \((a, b)\) was an arbitrary element of \(\mathbb{Z}_m \times \mathbb{Z}_n\), it follows that no element of \(\mathbb{Z}_m \times \mathbb{Z}_n\) has order \(mn\). Therefore, \(\mathbb{Z}_m \times \mathbb{Z}_n\) can’t be cyclic of order \(mn\), since a generator \textit{would} have order \(mn\).

\textbf{Remark.} More generally, if \(m_1, \ldots, m_k\) are pairwise relatively prime, then \(\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}\) is cyclic of order \(m_1 \cdots m_k\).

\textbf{Example. (Orders of elements in products)} \(\mathbb{Z}_5 \times \mathbb{Z}_6\) is cyclic of order 30. This means that as a group, it’s “the same as” \(\mathbb{Z}_{30}\). However, \(\mathbb{Z}_2 \times \mathbb{Z}_2\) is not cyclic of order 4.

Using an earlier remark, the element \((2, 4, 4)\) in \(\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_6\) has order \([2, 3, 3] = 6\) — because 2 has order 2 in \(\mathbb{Z}_4\), 4 has order 3 in \(\mathbb{Z}_{12}\), and 4 has order 3 in \(\mathbb{Z}_6\).

\textbf{Example. (A product of cyclic groups which is not cyclic)} \(\mathbb{Z}_2 \times \mathbb{Z}_4\) is a group of order \(2 \cdot 4 = 8\). However, it is \textit{not} cyclic of order 8, since \((2, 4) = 2 \neq 1\). In fact, if \((a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_4\), then

\[ 4(a, b) = (4a, 4b) = (0, 0). \]

Thus, every element of \(\mathbb{Z}_2 \times \mathbb{Z}_4\) has order less than or equal to 4. In particular, there can be no elements of order 8, i.e. no cyclic generators.

\(\textcopyright 2008\) by Bruce Ikenaga

6