Worksheet 3: Products

Definition. The **direct product** of the groups $(G_1, \star_1)$ and $(G_2, \star_2)$ is the group

$$G_1 \times G_2 = \{(x, y) \mid x \in G_1, y \in G_2\}$$

where the binary operation is $(x, y) \star (z, w) = (x \star_1 z, y \star_2 w)$.
The groups G_1 and G_2 are called the **factors** of G.

1. Practice with direct product groups.

   (a) List the elements of the group $\mathbb{Z}_2 \times \mathbb{Z}_2$, and then list the subgroup $\langle (x, y)\rangle$ generated by each element $(x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_2$. What is the order of every element in $\mathbb{Z}_2 \times \mathbb{Z}_2$? Is $\mathbb{Z}_2 \times \mathbb{Z}_2$ cyclic?

   The elements are:
   $$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}.$$

   The subgroup generated by each element is (the binary operation is adding coordinatewise mod 2):

   - $\langle (0, 0)\rangle = \{(0, 0)\}$
   - $\langle (0, 1)\rangle = \{(0, 0), (0, 1)\}$
   - $\langle (1, 0)\rangle = \{(0, 0), (1, 0)\}$
   - $\langle (1, 1)\rangle = \{(0, 0), (1, 1)\}$

   Because the order of any element is the size of the subgroup generated by that element, we just count the number of elements in each set above to find that:

   - $o(0, 0) = 1$
   - $o(0, 1) = 2$
   - $o(1, 0) = 2$
   - $o(1, 1) = 2$

   This group is **not cyclic** because there is no element (x, y) such that $\langle (x, y)\rangle = \mathbb{Z}_2 \times \mathbb{Z}_2$ (equivalently, there is no element (x, y) with $o(x, y) = 4 = |\mathbb{Z}_2 \times \mathbb{Z}_2|$).

   (b) List the elements of the group $\mathbb{Z}_2 \times \mathbb{Z}_3$, and then list the subgroup $\langle (x, y)\rangle$ generated by each element $(x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_3$. What is the order of every element in $\mathbb{Z}_2 \times \mathbb{Z}_3$? Is $\mathbb{Z}_2 \times \mathbb{Z}_3$ cyclic?

   The elements are:
   $$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}.$$

   The subgroup generated by each element is (the binary operation is adding mod 2 on the first coordinate and mod 3 on the second):

   - $\langle (0, 0)\rangle = \{(0, 0)\}$
   - $\langle (0, 1)\rangle = \{(0, 0), (0, 1), (0, 2)\}$
   - $\langle (0, 2)\rangle = \{(0, 0), (0, 1), (0, 2)\}$
   - $\langle (1, 0)\rangle = \{(0, 0), (1, 0)\}$
   - $\langle (1, 1)\rangle = \{(0, 0), (1, 1), (0, 2), (1, 0), (0, 1), (1, 2)\}$

- $\langle(1,2)\rangle = \{(0,0),(1,2),(0,1),(1,0),(0,2),(1,1)\}$

Because the order of any element is the size of the subgroup generated by that element, we just count the number of elements in each set above to find that:

- $o(0,0) = 1$
- $o(0,1) = 3$
- $o(0,2) = 3$
- $o(1,0) = 2$
- $o(1,1) = 6$
- $o(1,2) = 6$

This group is **cyclic** because $\langle(1,1)\rangle = \mathbb{Z}_2 \times \mathbb{Z}_3$ (equivalently, there exists an element (x,y) with $o(x,y) = 6 = |\mathbb{Z}_2 \times \mathbb{Z}_3|$).

(c) We could analogously define $G_1 \times G_2 \times \cdots \times G_k$ for k groups, instead of 2.

i. List the elements of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.
The elements are:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0,0),(0,0,1),(0,0,2),(0,1,0),(0,1,1),(0,1,2),(1,0,0),$$

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

ii. In general, if each group G_i has n_i elements, how many elements does the group $G = G_1 \times \cdots \times G_k$ have?
Because $G = \{(a_1, a_2, \ldots, a_k) \mid a_i \in G_i\}$ and there are $|G_i|$ choices for each coordinate a_i, the group G has $|G| = n_1 n_2 \ldots n_k = |G_1||G_2| \ldots |G_k|$ elements.

2. Let's prove some things:

(a) If $G = G_1 \times G_2$, prove that G is abelian if and only if each factor is abelian.
Homework!

(b) If $G = G_1 \times G_2$, and $x \in G_1$ and $y \in G_2$ have finite order, prove that

$$o(x,y) = \operatorname{lcm}(o(x), o(y)),$$

where lcm means *least common multiple.*

Then, check that this theorem gives you the same answer for the orders of the elements in $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$ in Problem 1.

Suppose n is any positive integer such that $(x,y)^n = (e_1, e_2)$ (which is the identity element in G). This implies that $(x^n, y^n) = (e_1, e_2)$, or $x^n = e_1$ and $y^n = e_2$. Therefore, n must be a multiple of both $o(x)$ and $o(y)$. The smallest such positive integer is $\operatorname{lcm}(o(x), o(y))$, so $o(x,y) \leq \operatorname{lcm}(o(x), o(y))$. Futhermore, if $n = o(x,y) < \operatorname{lcm}(o(x), o(y))$, by definition, it is not a common multiple of both $o(x)$ and $o(y)$, so it is not possible that both $x^n = e_1$ and $y^n = e_2$. Therefore, we must have $n = o(x,y) = \operatorname{lcm}(o(x), o(y))$.

This matches the orders from problem 1:

For $\mathbb{Z}_2 \times \mathbb{Z}_2$, we have:

- $o(0,0) = 1 = \operatorname{lcm}(1,1)$
- $o(0,1) = 2 = \operatorname{lcm}(1,2)$

- $o(1,0) = 2 = \text{lcm}(2,1)$
- $o(1,1) = 2 = \text{lcm}(2,2)$

and for $\mathbb{Z}_2 \times \mathbb{Z}_3$ we have:

- $o(0,0) = 1 = \text{lcm}(1,1)$
- $o(0,1) = 3 = \text{lcm}(1,3)$
- $o(0,2) = 3 = \text{lcm}(1,3)$
- $o(1,0) = 2 = \text{lcm}(2,1)$
- $o(1,1) = 6 = \text{lcm}(2,3)$
- $o(1,2) = 6 = \text{lcm}(3,2)$

(c) If $G = G_1 \times G_2$, and G_1 and G_2 are cyclic groups of finite order, prove that G is cyclic if and only if $|G_1|$ and $|G_2|$ are relatively prime.

We use the following fact, which we proved earlier in the semester: a group G is cyclic if and only if there exists an element of G with order equal to $|G|$.

First, suppose G_1 and G_2 are cyclic groups with $|G_1|$ and $|G_2|$ relatively prime. Then, there exist $x \in G_1$ and $y \in G_2$ with $o(x) = |G_1|$ and $o(y) = |G_2|$, so by the previous problem,

$$o(x,y) = \text{lcm}(o(x), o(y)) = \text{lcm}(|G_1|, |G_2|).$$

Because $|G_1|$ and $|G_2|$ are relatively prime, their least common multiple is their product $|G_1||G_2| = |G|$, so

$$o(x,y) = |G_1||G_2| = |G|.$$

Therefore, the element (x,y) has order equal to $|G|$, so G is cyclic.

Now, suppose $|G|$ is cyclic. Then, there exists an element $(x,y) \in G$ such that $o(x,y) = |G|$. However, this means

$$o(x,y) = \text{lcm}(o(x), o(y)) = |G| = |G_1||G_2|.$$

Because $o(x) \leq |G_1|$ and $o(y) \leq |G_2|$, this is only possible if $o(x) = |G_1|$ and $o(y) = |G_2|$, so G_1 and G_2 are cyclic, and $\text{lcm}(o(x), o(y)) = \text{lcm}(|G_1|, |G_2|) = |G_1||G_2|$. This implies that $|G_1|$ and $|G_2$ are relatively prime.

(d) Generalize (a), (b), and (c) to direct products $G_1 \times G_2 \times \cdots \times G_k$.

The relevant theorems are: (and they can be proved either directly or by induction)

Theorem. Suppose $G = G_1 \times G_2 \times \cdots \times G_k$. Then, G is abelian if and only if each G_i is abelian.

Theorem. Suppose $G = G_1 \times G_2 \times \cdots \times G_k$ and $(x_1, x_2, \ldots, x_k) \in G$ such that $o(x_i)$ is finite for each x_i. Then,

$$o(x_1, x_2, \ldots, x_n) = \text{lcm}(o(x_1), o(x_2), \ldots, o(x_n)).$$

Theorem. Suppose $G = G_1 \times G_2 \times \cdots \times G_k$ and each G_i is a finite group. Then, G is cyclic if and only if each G_i is cyclic and the orders $|G_i|$ are relatively prime.

3. Some applications of the theorems:

(a) Prove that $G = D_3 \times \mathbb{Z}_4$ is not abelian.
By 2(a), G is not abelian because D_3 is not abelian.

(b) Prove that $G = \mathbb{Z}_3 \times \mathbb{Z}_8$ is cyclic, and find an element $(x, y) \in G$ that is a generator.
By 2(c), G is cyclic because 3 and 8 are relatively prime. A generator is an element (x, y) with $o(x, y) = |G| = 3 \cdot 8 = 24$, and by 2(b) this must be an element (x, y) with $x \in \mathbb{Z}_3$ of order 3 and $y \in \mathbb{Z}_8$ of order 8. Any element $(x, y) \in G$ with $o(x) = 3$ and $o(y) = 8$ will work, such as: $(1, 1)$ or $(2, 5)$ or $(1, 7)$ or ... (more answers possible).

(c) Find the order of $(2, 3, 4) \in \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_9$.
By 2(b), $o(2, 3, 4) = \text{lcm}(o(2), o(3), o(4)) = \text{lcm}(3, 5, 9) = 45$.

(d) Is $G = \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_9$ cyclic?
By 2(b) or its generalization, for any element $(x, y, z) \in G$, $o(x, y, z) = \text{lcm}(o(x), o(y), o(z))$. Because $x \in \mathbb{Z}_3$, the possible orders of x are 1 or 3. Because $y \in \mathbb{Z}_5$, the possible orders of y are 1 or 5. Because $z \in \mathbb{Z}_9$, the possible orders of z are $1, 3$, or 9. Therefore, the possible orders of (x, y, z) are:

$$o(x, y, z) = \text{lcm}(o(x), o(y), o(z))$$

where

- $\text{lcm}(o(x), o(y), o(z)) = \text{lcm}(1, 1, 1) = 1$
- $\text{lcm}(o(x), o(y), o(z)) = \text{lcm}(1, 1, 3) = 3$
- $\text{lcm}(o(x), o(y), o(z)) = \text{lcm}(1, 1, 9) = 9$
- $\text{lcm}(o(x), o(y), o(z)) = \text{lcm}(1, 5, 1) = 5$
- $\text{lcm}(o(x), o(y), o(z)) = \text{lcm}(1, 5, 3) = 15$
- $\text{lcm}(o(x), o(y), o(z)) = \text{lcm}(1, 5, 9) = 45$
- $\text{lcm}(o(x), o(y), o(z)) = \text{lcm}(3, 1, 1) = 3$
- $\text{lcm}(o(x), o(y), o(z)) = \text{lcm}(3, 1, 3) = 3$
- $\text{lcm}(o(x), o(y), o(z)) = \text{lcm}(3, 1, 9) = 9$
- $\text{lcm}(o(x), o(y), o(z)) = \text{lcm}(3, 5, 1) = 15$
- $\text{lcm}(o(x), o(y), o(z)) = \text{lcm}(3, 5, 3) = 15$
- $\text{lcm}(o(x), o(y), o(z)) = \text{lcm}(3, 5, 9) = 45$

None of these orders are equal to the size of G, which is $|G| = 3 \cdot 5 \cdot 9 = 135$, so G cannot be cyclic.
(Alternatively, you can use the generalization of 2(c) that G is not cyclic because the orders of $\mathbb{Z}_3$ and $\mathbb{Z}_9$ are not relatively prime.)

(e) Is Is $G = \mathbb{Z}_9 \times \mathbb{Z}_{17} \times \mathbb{Z}_{200}$ cyclic?
By 2(b)/its generalization, $o(1, 1, 1) = \text{lcm}(o(1), o(1), o(1)) = 9 \cdot 17 \cdot 200 = |G|$, so G has an element of order $|G|$, so G is cyclic.

(f) Find an abelian group G with 12 elements where every element has order at most 6.
The group $\mathbb{Z}_2 \times \mathbb{Z}_6$ satisfies this. It is abelian by 2(a), and for any $(x, y) \in G$, $o(x, y) = \text{lcm}(o(x), o(y))$, and $o(x)$ is 1 or 2 and $o(y)$ is $1, 2, 3$ or 6, so the least common multiple is always at most 6.

(g) Find a non-abelian group G with 12 elements where every element has order at most 6.

The group $\mathbb{Z}_2 \times D_3$ satisfies this. It is not abelian by 2(a), and the orders of elements in $\mathbb{Z}_2$ are 1 or 2 and the orders of elements in D_3 are $1, 2$ or 3, so the least common multiple of the order of an element in $\mathbb{Z}_2$ and one in D_3 is $1, 2, 3$, or 6. Therefore, by 2(b), every element has order at most 6.

(h) Find an abelian group G with 24 elements where every element has order at most 6.

The group $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6$ satisfies this by the same reasoning as 3(f).

(i) Find a non-abelian group G with 24 elements where every element has order at most 6.

Homework!