

11. DIRECT PRODUCT

The **Cartesian product** of sets $S_1 \times S_2 \times \cdots \times S_n$ is the set of all ordered n -tuples (x_1, x_2, \cdots, x_n) where $x_i \in S_i$.

Question: How many elements does $S_1 \times S_2 \times \cdots \times S_n$ have?

Definition 11.1. If G_1, \cdots, G_n are groups then the **direct product**

$$G_1 \times G_2 \times \cdots \times G_n$$

is the group of all ordered n -tuples (a_1, \cdots, a_n) under coordinate-wise multiplication:

$$(a_1, \cdots, a_n)(b_1, \cdots, b_n) = (a_1b_1, \cdots, a_nb_n)$$

This may be more familiar when the group operation is addition:

$$(a_1, \cdots, a_n) + (b_1, \cdots, b_n) = (a_1 + b_1, \cdots, a_n + b_n)$$

In the additive case, when n is finite, the direct product of additive groups is called the **direct sum** and is sometimes written

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n.$$

For example:

$$\mathbb{Z} \times \mathbb{Z} = \mathbb{Z} \oplus \mathbb{Z}$$

Problem: If $g \in G$ has order 4 and $h \in H$ has order 6 then show that the element $(g, h) \in G \times H$ has order 12 (the least common multiple of 4 and 6).

Problem: If $o(g) = n$ and $o(h) = m$ are relatively prime then show that (g, h) has order nm .

Theorem 11.2. If n, m are relatively prime then $\mathbb{Z}_n \times \mathbb{Z}_m$ is a cyclic group of order nm . I.e.,

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$$

where \cong means isomorphic.

The rest of this section will be covered by Bong Lian next week.

Also, we will skip section 12. A more useful application of group theory is RSA: You choose a group G , write your message as an element $g \in G$ and raise it to a power, say g^3 . This is the coded form of your message. It is impossible to find the cube root of g^3 without knowing the order of the group. For example, if you know that your group has order 220 then you just raise to the 147-th power to get the original message:

$$(g^3)^{147} = g^{441} = (g^{220})^2 g = g.$$

The time it takes to raise to the n -th power is on the order of $\log n$.