Lecture Notes: Abstract Algebra — (Course By: Alvaro Lozano-Robledo)

Thobias K. Høivik

March 14, 2025

Example

$\mathbb{Z}/_2\mathbb{Z} \times \mathbb{Z}/_2\mathbb{Z} = \{(a \bmod 2, b \bmod 2) | a, b \in \{0, 1\}\}$

Proposition 1. *Let $< G, \star_G >, < H, \star_H >$ be groups. Define $< G \times H, \star >= \{(g, h) | g \in G \wedge h \in H\}$ with $(g, h) \star (g', h') = (g \star_G g', h \star_H h')$. Then $< G \times H, \star >$ is a group (external indirect product of G & H).*

Proof.

- $\star$ is closed:

Let $g, g' \in G \wedge h, h' \in H$.

$$(g, h) \star (g', h') = (g \star_G g', h \star_H h')$$

$$\begin{aligned} g, g' \in G \wedge h, h' \in H &\Rightarrow g \star_G g' \in G \wedge h \star_H h' \in H \\ &\Rightarrow (g \star_G g', h \star_H h') \in G \times H \end{aligned}$$

meaning $G \times H$ is closed under $\star$.

- Identity:

(e_G, e_H) is the identity as $\star$ is applying the respective binary operations of G and H componentwise and we know

$$(e_G \star_G g, e_H \star_H h) = (g \star_G e_G, h \star_H e_H) = (g, h)$$

So there exists an identity element of $G \times H$.

- Inverses:

Since G and H are groups, every $g \in G$ has an inverse $g^{-1} \in G$, and every $h \in H$ has an inverse $h^{-1} \in H$. Define the inverse of $(g, h) \in G \times H$ as (g^{-1}, h^{-1}). Then:

$$(g, h) \star (g^{-1}, h^{-1}) = (g \star_G g^{-1}, h \star_H h^{-1}) = (e_G, e_H)$$

$$(g^{-1}, h^{-1}) \star (g, h) = (g^{-1} \star_G g, h^{-1} \star_H h) = (e_G, e_H)$$

So every element in $G \times H$ has an inverse.

- Associativity:

Since $\star_G$ and $\star_H$ are associative, for all $g, g', g'' \in G$ and $h, h', h'' \in H$,

$$((g,h) \star (g',h')) \star (g'',h'') = (g \star_G g', h \star_H h') \star (g'',h'')$$

$$= ((g \star_G g') \star_G g'', (h \star_H h') \star_H h'')$$

$$= (g \star_G (g' \star_G g''), h \star_H (h' \star_H h'')) \quad \text{(since } \star_G \text{ and } \star_H \text{ are associative)}$$

$$= (g,h) \star (g' \star_G g'', h' \star_H h'') = (g,h) \star ((g',h') \star (g'',h''))$$

Thus, $\star$ is associative.
Since $\star$ satisfies closure, identity, inverses, and associativity, $G \times H$ is a group. □

The Order of Elements in $G \times H$

Theorem 1. *Let G and H be groups, $g \in G, h \in H$ of finite orders $|g| = r, |h| = s$. Then, $|(g,h)| = lcm(r,s)$.*

Proof. Let $n = |(g,h)|, m = lcm(r,s)$. Then,

$$(g,h)^m = (g^m, h^m)$$

note that

$$lcm(r,s) = m \Rightarrow m = rk = sj \text{ where } s, j \in \mathbb{Z}$$

so

$$(g^m, h^m) = ((g^r)^k, (h^s)^j) = ((e_G)^k, (e_H)^j) = (e_G, e_H)$$

thus

$$n \leq m$$

Also

$$(g,h)^n = e, g^n = e \wedge h^s = e \Rightarrow r \mid n \wedge s \mid n$$

$$\Rightarrow lcm(r,s) \mid n \rightarrow m \leq n$$

Since $m \leq n \wedge n \leq m$ we have $m = n$, completing the proof.

□