Math 403 Chapter 8: External Direct Products

---

1. **Introduction:** The idea of this chapter is to discuss how we can combine groups to form other groups. The reason for doing this is also to see the reverse, that a complicated group could possibly be broken down into a combination of simpler groups.

2. **Definition:** Given two group G and H we define the *external direct product* $G \oplus H$ to be the group whose set is:
$$\{(g,h) \mid g \in G, h \in H\}$$
and whose operation is:
$$(g_1,h_1) * (g_2,h_2) = (g_1 *_G g_2, h_1 *_H h_2)$$
This definition may be expanded to an arbitrary number of groups.

   Example: Consider $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. This is the group with set:
$$\{(0,0),(1,0),(0,1),(1,1)\}$$
and a sample operation would be:
$$(1,0)+(1,1)=(0,1)$$

   Example: Consider $U(10) \oplus U(5)$. This is the group with set:
$$\{(1,1),(1,2),(1,3),(1,4),(3,1),(3,2),(3,3),(3,4),$$
$$(7,1),(7,2),(7,3),(7,4),(9,1),(9,2),(9,3),(9,4)\}$$
and a sample operation would be:
$$(3,3)(7,4)=(1,2)$$

3. **Properties of External Direct Products:**

   (a) **Theorem:** We have:
$$|(g,h)| = \text{lcm }(|g|,|h|)$$

   Proof: Put $L = \text{lcm}\,(|g|,|h|)$. Since L is a multiple of each we know $L = \alpha|g|$ and $L = \beta|h|$ for $\alpha, \beta \in \mathbb{Z}$. Observe that:
$$(g,h)^L = \left(g^L, h^L\right) = \left(\left(g^{|g|}\right)^{\alpha}, \left(h^{|h|}\right)^{\beta}\right) = (e_G, e_H)$$
which tells us that:
$$L = \text{lcm}\,(|g|,|h|) \geq |(g,h)|$$
However we also know that:
$$(e_G,e_H) = (g,h)^{|(g,h)|} = \left(g^{|(g,h)|}, h^{|(g,h)|}\right)$$
So that $|(g,h)|$ is a common multiple of $|g|$ and $|h|$ and so:
$$|(g,h)| \geq \text{lcm}\,(|g|,|h|)$$

   $\mathcal{QED}$

(b) **Theorem:** If G and H are finite cyclic groups then $G \oplus H$ is cyclic iff $|G|$ and $|H|$ are coprime.

Proof: Suppose $|G| = m$ and $|H| = n$. Then we know $|G \oplus H| = mn$.

$\Rightarrow$: We assume $G \oplus H$ is cyclic and claim coprimality. Since $G \oplus H$ is cyclic we can find some $(g,h) \in G \oplus H$ with $\langle (g,h) \rangle = G \oplus H$ so that $|(g,h)| = mn$. Let $d = \gcd(m,n)$ and then since:

$$(g,h)^{mn/d} = \left((g^m)^{n/d}, (h^n)^{m/d}\right) = \left(e^{n/d}, e^{m/d}\right) = (e,e)$$

we know that $mn/d \geq mn$ (since mn is the order, the least power that gives the identity) and so $d = 1$.

$\Leftarrow$: We assume $G = \langle g \rangle$ and $H = \langle h \rangle$ and suppose $\gcd(m,n) = 1$. Then by the previous theorem we have:

$$|(g,h)| = \operatorname{lcm}(|g|, |h|) = \operatorname{lcm}(m,n) = \frac{mn}{\gcd(m,n)} = mn$$

and so $G \oplus H$ is cyclic. $\mathcal{QED}$

4. **Theorem (Ramifications for $\mathbb{Z}$):**

We have $\mathbb{Z}_m \oplus \mathbb{Z}_n \approx \mathbb{Z}_{mn}$ iff $\gcd(m,n) = 1$.

Proof: We know $\mathbb{Z}_m$ and $\mathbb{Z}_n$ are cyclic and so this follows immediately from the previous theorem. $\mathcal{QED}$

Example: We can break down groups using prime factorizations, for example we know that:

$$\mathbb{Z}_{100} \approx \mathbb{Z}_4 \oplus \mathbb{Z}_{25}$$

Note: We can't break these apart without coprimality, for example

$$\mathbb{Z}_4 \not\approx \mathbb{Z}_2 \oplus \mathbb{Z}_2$$