MARCH 14 NOTES

1. Section 6: Direct Products

Definition 1.1. Suppose $(G_1, \star_1)$ and $(G_2, \star_2)$ are groups. The **direct product** of G_1 and G_2 is the group

$$G_1 \times G_2 = \{(a, b) \mid a \in G_1, b \in G_2\}$$

where the binary operation is $(a, b) \star (c, d) = (a \star_1 c, b \star_2 d)$.

This is a group: the binary operation is associative since $\star_1$ and $\star_2$ are. There is an identity (e_1, e_2), where e_i is the identity in G_i, because $(a, b) \star (e_1, e_2) = (a \star_1 e_1, b \star_2 e_2) = (a, b)$. Finally, there are inverses: $(a, b)^{-1} = (a^{-1}, b^{-1})$ because $(a, b) \star (a^{-1}, b^{-1}) = (a \star_1 a^{-1}, b \star_2 b^{-1}) = (e_1, e_2)$.

Example 1.2. List the elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$. Is this group cyclic?

The elements are $(0, 0), (0, 1), (1, 0), (1, 1)$. This group is not cyclic because each element has order ≤ 2: $o(0, 0) = 1$ because $(0, 0)$ is the identity; $o(0, 1) = 2$ because $(0, 1) + (0, 1) = (0, 0)$; similarly $o(1, 0) = 2$ and $o(1, 1) = 2$. Because each element has order 2, none of the elements can generate the whole group, so the group is not cyclic.

Example 1.3. List the elements of $\mathbb{Z}_2 \times \mathbb{Z}_3$. Is this group cyclic?

The elements are $(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)$. This group *is* cyclic because it can be generated by $(1, 1)$:

$$1\cdot(1, 1) = (1, 1), \quad 2\cdot(1, 1) = (0, 2), \quad 3\cdot(1, 1) = (1, 0), \quad 4\cdot(1, 1) = (0, 1), \quad 5\cdot(1, 1) = (1, 2), \quad 6\cdot(1, 1) = (0, 0)$$

so $o(1, 1) = 6$ and $\langle(1, 1)\rangle = \mathbb{Z}_2 \times \mathbb{Z}_3$.

Theorem 1.4. *Let $G = G_1 \times G_2$. If $g_1 \in G_1$, $g_2 \in G_2$ and $o(g_1) = n_1$ and $o(g_2) = n_2$, then $o((g_1, g_2)) = \text{lcm}(n_1, n_2)$.*

Proof. Suppose $n = o(g_1, g_2)$ so $(g_1, g_2)^n = (e_1, e_2)$. Then, $(g_1^n, g_2^n) = (e_1, e_2)$ so $n_1 = o(g_1) \mid n$ and $n_2 = o(g_2) \mid n$, so $\text{lcm} n_1 n_2 \mid n$. Conversely, if $m = \text{lcm}(n_1, n_2)$, then $m = k_1 n_1$ and $m = k_2 n_2$ for some k_1, k_2 and therefore $(g_1, g_2)^m = (g_1^m, g_2^m) = (g_1^{k_1 n_1}, g_2^{k_2 n_2}) = (e_1, e_2)$, so $n \leq \text{lcm}(n_1, n_2)$. Therefore, we must have $n = \text{lcm}(n_1, n_2)$. $\square$

Corollary 1.5. If $G = G_1 \times G_2$ is a product of cyclic groups with $|G_1| = n_1$ and $|G_2| = n_2$, then G is cyclic if and only if $\gcd(n_1, n_2) = 1$.

Proof. Recall that G is cyclic if and only if there exists an element of G with $o(g) = |G| = n_1 n_2$. For $g = (g_1, g_2) \in G$, $o(g) = \text{lcm}(o(g_1), o(g_2))$. If G is cyclic, then there exists an element $(g_1, g_2) \in G$ that generates G and $o(g_1, g_2) = |G| = n_1 n_2$. This implies that every element of G can be written as $(g_1, g_2)^n$ for some n, so in particular every element of G_1 can be written as a power of g_1 and every element of G_2 can be written as a power of g_2. Therefore, g_1 generates G_1 and g_2 generates G_2, so $o(g_1) = n_1$ and $o(g_2) = n_2$. Therefore, $n_1 n_2 = o(g_1, g_2) = \text{lcm}(o(g_1), o(g_2)) = \text{lcm}(n_1, n_2)$, which happens if and only if $\gcd(n_1, n_2) = 1$.

For the converse, if $\gcd(n_1, n_2) = 1$, let g_1 be a generator of G_1 and g_2 be a generator of G_2. Then, $o(g_1) = n_1$ and $o(g_2) = n_2$, so $o(g_1, g_2) = \text{lcm}(o(g_1), o(g_2)) = \text{lcm}(n_1, n_2) = n_1 n_2$, so $(g_1, g_2) \in G$ is an element of order $n_1 n_2 = |G|$, and therefore G is cyclic. $\square$

We can construct direct products of more groups (e.g. $G_1 \times G_2 \times G_3 \times \ldots$) and these theorems will still hold. In general:

Definition 1.6. Suppose $(G_1, \star_1)$, $(G_2, \star_2)$, ..., $(G_k, \star_k)$ are groups. The **direct product** of these groups is the group

$$G_1 \times G_2 \times \cdots \times G_k = \{(a_1, a_2, \ldots, a_k) \mid a_i \in G_i\}$$

where the binary operation is $(a_1, a_2, \ldots, a_k) \star (b_1, b_2, \ldots, b_k) = (a_1 \star_1 b_1, a_2 \star_2 b_2, \ldots, a_k \star_k b_k)$.

Theorem 1.7. *Let $G = G_1 \times G_2 \times \cdots \times G_k$. If $g_i \in G_i$ has $o(g_i) = n_i$ for each i, then $o((g_1, g_2, \ldots, g_k)) = \operatorname{lcm}(n_1, n_2, \ldots, n_k)$.*

Corollary 1.8. If $G = G_1 \times G_2 \times \cdots \times G_k$ is a product of cyclic groups with $|G_i| = n_i$, then G is cyclic if and only if $\gcd(n_i, n_j) = 1$ for all $i \neq j$.