PMATH 336: INTRODUCTION TO GROUP THEORY WITH APPLICATIONS
NOTES FOR WEEK 7

INSTRUCTOR: ARUNDHATHI KRISHNAN

8. Direct products

8.1. Definition of external direct products and examples.

Definition 8.1.1. The external direct product of groups $G_1, \ldots, G_n$, written as $G_1 \oplus \cdots \oplus G_n$, is the set of all n-tuples in which the i-th component is an element of G_i, and the operation is component-wise.

That is,

$$G_1 \oplus \cdots \oplus G_n = \{(g_1, \ldots, g_n) \mid g_i \in G_i\}$$

with $(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1h_1, \ldots, g_nh_n)$.

It is implicit in the definition that the operation in each component i corresponds to the binary operation of G_i. It is an easy exercise to show that the external direct product of groups is itself a group.

Example 8.1.2.

(i)
$$U(5) \oplus U(3) = \{(1,1),(1,2),(2,1),(2,2),(3,1),(3,2),(4,1),(4,2)\}$$
with a sample product given by, say, $(2,2)(3,1) = (1,2)$ as $2 \cdot 3 \mod 5 = 1$ and $2 \cdot 1 \mod 3 = 2$.

(ii)
$$\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}.$$
It turns out that this group, which is Abelian and of order 6 is isomorphic to $\mathbb{Z}_6$. To see this, we show that $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is cyclic of order 6. Consider the element $(1,1)$ in the direct product. Then
$$\begin{array}{lll} 1(1,1) = (1,1) & 2(1,1) = (0,2) & 3(1,1) = (1,0) \\ 4(1,1) = (0,1) & 5(1,1) = (1,2) & 6(1,1) = (0,0) \end{array}.$$
Hence $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is cyclic of order 6 and is isomorphic to $\mathbb{Z}_6$.

(iii) Any group of order 4 is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Let $G = \{e, a, b, ab\}$. If G is cyclic, it is isomorphic to $\mathbb{Z}_4$. If not, by Lagrange's theorem it holds that each non-identity element has order 2, that is, $|\,a\,| = |\,b\,| = |\,ab\,| = 2$. Define the mapping $\varphi : G \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$ by $\varphi(e) = (0,0), \varphi(a) = (1,0), \varphi(b) = (0,1)$ and $\varphi(ab) = (1,1)$. Then it is easily verified that φ is an isomorphism.

Note that combining this example with Theorem 7.2.11 gives a complete classification of all groups of order $2p$ for p prime.

8.2. **Properties of external direct products.**

Theorem 8.2.1. *The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components of the element. That is,*

$$|\,(g_1, g_2, \ldots, g_n)\,| = \text{lcm}(|\,g_1\,|, |\,g_2\,|, \ldots, |\,g_n\,|).$$

Proof. Let e_i denote the identity of G_i for each $i = 1, \ldots, n$, and $s = \text{lcm}(|\,g_1\,|, \ldots, |\,g_n\,|)$ and $t = |\,(g_1, \ldots, g_n)\,|$. Then $(g_1, \ldots, g_n)^s = (g_1^s, \ldots, g_n^s) = (e_1, \ldots, e_n)$, so that t divides s by Corollary 4.1.5.

On the other hand, as $(g_1^t, \ldots, g_n^t) = (g_1, \ldots, g_n)^t = (e_1, \ldots, e_n)$, we have $g_i^t = e_i$ for each i. By another application of Corollary 4.1.5, this gives that $|\,g_i\,|$ divides t for each i, hence s – the least common multiple of all the $|\,g_i\,|$ – divides t.

Altogether we get that $s = t$ as required. □

Example 8.2.2.

(i) We determine the number of elements in $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$ of order 5. By Theorem 8.2.1, we must count those elements $(a, b) \in \mathbb{Z}_{25} \oplus \mathbb{Z}_5$ such that $5 = \text{lcm}(|\,a\,|, |\,b\,|)$. Hence we must have either $|\,a\,| = 5$ and $|\,b\,| = 1$ or 5, or $|\,a\,| = 1$ and $|\,b\,| = 5$.

In the first case, a may be $5, 10, 15$ or 20 (this follows from Corollary 4.1.10). The element b may be 0 (if its order is 1) or one of $1, 2, 3, 4$ (if its order is 5). Hence there are 4 choices of a and 5 for b with a total of 20 choices.

In the second case, a must be 0, whereas b may be one of $1, 2, 3, 4$. Hence this case gives 4 elements of order 5.

Altogether, there are 24 elements of order 5 in $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$.

(ii) We determine the number of cyclic subgroups in $\mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$ of order 10.

Let us, like in the previous example, enumerate the number of elements of order 10. Using Theorem 8.2.1, this means we enumerate elements (a, b) with $a \in \mathbb{Z}_{100}, b \in \mathbb{Z}_{25}$ and $\text{lcm}(|\,a\,|, |\,b\,|) = 10$. This means that either $|\,a\,| = 10$ and $|\,b\,| = 1$ or 5; or $|\,a\,| = 2$ and $|\,b\,| = 5$. In the first case we get 4 choices for a $(10, 30, 70, 90)$ and 5 for b (0 if $|\,b\,| = 1$ and $5, 10, 15, 20$ if $|\,b\,| = 5$. In the second case, we get one choice of a $(a = 1)$ and four choices for b. Hence we get a total of 24 elements of order 10. However, as each cyclic subgroup of order 10 has 4 generators, this means that there is a total of 6 cyclic subgroups of order 10.

Theorem 8.2.3. *Let G and H be finite cyclic groups. Then $G \oplus H$ is cyclic if and only if $|\,G\,|$ and $|\,H\,|$ are relatively prime.*

Proof. Suppose $G \oplus H$ is cyclic and $m = |\,G\,|, n = |\,H\,|$. Let $d = \gcd(m, n)$. Then $|\,G \oplus H\,| = |\,G\,|\,|\,H\,| = mn$. Suppose (a, b) is a generator of $G \oplus H$. Now, $(a, b)^{\frac{mn}{d}} = ((a^m)^{\frac{n}{d}}, (b^n)^{\frac{m}{d}}) = (e_G, e_H)$ as $a^m = e_G, b^n = e_H$, m and n being the orders of G and H respectively. Hence $mn = |\,(a, b)\,|$ divides $\frac{mn}{d}$ which forces that $d = 1$.

On the other hand, suppose $\gcd(m, n) = 1$ and a, b are generators of G and H respectively. Then $|\,(a, b)\,| = \text{lcm}(m, n) = mn = |\,G \oplus H\,|$ (as $\gcd(m, n) = 1$), so that (a, b) must be a generator of $G \oplus H$. □

The following corollary follows by induction applied to Theorem 8.2.3.

Corollary 8.2.4. *An external direct product $G_1 \oplus \cdots \oplus G_n$ of finite cyclic groups is cyclic if and only if $|\,G_i\,|$ and $|\,G_j\,|$ are relatively prime for all $i \neq j$.*

Corollary 8.2.5. *Let $m = n_1 \cdots n_k$. Then $\mathbb{Z}_m$ is isomorphic to $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ if and only if $\gcd(n_i, n_j) = 1$ for all $i \neq j$.*

The above results can be used to express the same group up to isomorphism in different forms. For example,

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{15} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{30}.$$

We also have

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{10}.$$

8.3. **Internal Direct Products.** Why do we use the term "external" for the direct products we considered so far? We start with a finite number of groups and use them to arrive at a larger group in such a way that properties of the larger group can be derived from them. For instance, if $G = H \oplus K$, then $|\,G\,| = |\,H\,|\,|\,K\,|$; every element of G has the form (h, k) with $h \in H, k \in K$; if $|\,h\,|$ and $|\,k\,|$ are finite, then $|\,(h, k)\,| = \text{lcm}(|\,h\,|, |\,k\,|)$; if H and K are Abelian, then so is $G = H \oplus K$; if H and K are cyclic and $\gcd(|\,H\,|, |\,K\,|) = 1$, then $G = H \oplus K$ is also cyclic.

We would now like to reverse this process, that is, to start with a group G and break it down into a product of subgroups so that properties of G can be obtained from properties of the subgroups. It is possible to do this if the subgroups are *normal*.

Definition 8.3.1. A subgroup H of a group G is called a normal subgroup of G if $aH = Ha$ for all $a \in G$. This is denoted by $H \trianglelefteq G$.

We will say a lot more about normal subgroups next week, but for the time being, we consider how they play a part in internal direct products.

Proposition 8.3.2. *Let H be a normal subgroup of a group G and K be any subgroup of G. Then $HK = \{hk \mid h \in H, k \in K\}$ is a subgroup of G.*

Proof. The identity $e = ee \in HK$, so HK is non-empty. let $a = h_1k_1, b = h_2k_2 \in HK$. Then $ab^{-1} = (h_1k_1)(k_2^{-1}h_2^{-1}) = h_1(k_1k_2^{-1})h_2^{-1} = h_1h'(k_1k_2^{-1})$ for some $h' \in H$ as H is normal. Hence $ab^{-1} = (h_1h')(k_1k_2^{-1}) \in HK$ so that HK is a subgroup. □

Definition 8.3.3. A group G is said to be the internal direct product of H and K and we write $G = H \times K$ if H and K are normal subgroups of G and

$$G = HK,\ H \cap K = \{e\}.$$

Exercise 8.3.4. Let $G = D_6 = \{r_0, \ldots, r_5, s_0, \ldots, s_5\}$ the dihedral group of order 12. Let $H = \{r_0, r_2, r_4, s_0, r_2s_0, r_4s_0\}$ and $K = \{r_0, r_3\}$. Then verify that H and K are normal subgroups of G, $H \cap K = \{r_0\}$ and $HK = G$.

Definition 8.3.5. Let $H_1, H_2, \ldots, H_n$ be a finite collection of normal subgroups of G. We say that G is the internal direct product of $H_1, H_2, \ldots, H_n$ and write $G = H_1 \times H_2 \times \cdots \times H_n$, if

(i) $G = H_1H_2 \cdots H_n = \{h_1h_2 \cdots h_n \mid h_i \in H_i\}$,
(ii) $(H_1H_2 \cdots H_i) \cap H_{i+1} = \{e\}$ for $i = 1, 2, \ldots, n-1$.

Theorem 8.3.6. *If a group G is the internal direct product of a finite number of subgroups $H_1, H_2, \ldots, H_n$, then G is isomorphic to the external direct product of $H_1, H_2, \ldots, H_n$.*

Proof. We first show that $h_i \in H_i$ and $h_j \in H_j$ commute for $i \neq j$ as

$$(h_ih_jh_i^{-1})h_j^{-1} \in H_jh_j^{-1} = H_j,$$

as H_j is normal and

$$h_i(h_j h_i^{-1} h_j^{-1}) \in h_i H_i = H_i,$$

as H_i is normal.

Hence $h_i h_j h_i^{-1} h_j^{-1} \in H_i \cap H_j = \{e\}$, so that $h_i h_j = h_j h_i$.

Next, we show that each element of G has a unique representation in the form $h_1 h_2 \cdots h_n$ with $h_i \in H_i$. Indeed, suppose $h_1 h_2 \cdots h_n = h_1' h_2' \cdots h_n'$ with $h_i, h_i' \in H_i$ for each i. Then $h_n' h_n^{-1} = (h_{n-1}')^{-1} \cdots (h_1')^{-1} h_1 \cdots h_{n-1}$. By the fact that h_i and h_j commute for $i \neq j$, we get $h_n' h_n^{-1} = (h_1')^{-1} h_1 (h_2')^{-1} h_2 \cdots (h_{n-1}')^{-1} h_{n-1}$, so that $h_n' h_n^{-1} \in H_n \cap H_1 H_2 \cdots H_{n-1} = \{e\}$ and $h_n' = h_n$. We can now cancel h_n and h_n' from the two sides of $h_1 \cdots h_n = h_1' \cdots h_n'$ and repeat the same process until we arrive at $h_i = h_i'$ for all i.

Now that we have established the uniqueness of the representation of an element g in G as a product of elements of H_i we can define the following map $\varphi : G \to H_1 \oplus H_2 \oplus \cdots \oplus H_n$ without ambiguity:

$$\varphi(h_1 h_2 \cdots h_n) = (h_1, h_2, \cdots, h_n).$$

Then φ is an isomorphism (verify this!). □

We will return to some consequences of this theorem next week.

References

[1] Chapters 8, 9. Gallian, Joseph. Contemporary abstract algebra. Nelson Education, 2012.