Math 375
Week 8

1.1 (External) Direct Products

Consider the following general situation: let G and H be two sets (not necessarily distinct). Consider the set of pairs

$$G \times H = \{(g,h) |\ g \in G,\ h \in H\}.$$

This set is usually called the **(external) direct product** of G and H. A familiar example is $\mathbf{R} \times \mathbf{R}$ which we usually write as $\mathbf{R}^2$. When both G and H are groups, there is a natural way to add or multiply elements of such a set together: simply add or multiply componentwise, just as we do in $\mathbf{R}^2$.

$$(g_1,h_1)(g_2,h_2) = (g_1g_2, h_1h_2)$$

where the first product is computed in G and the second in H. Notice that this is a binary operation on $G \oplus H$.

THEOREM 0 *$G \oplus H$ is a group using the operation above and is usually denoted by $G \oplus H$.*

PROOF (i) Closure: Given $(g_1,h_1),\ (g_2,h_2) \in G \oplus H$,

$$(g_1,h_1)(g_2,h_2) = (g_1g_2, h_1h_2) \in G \oplus H.$$

(ii) Associativity:

$$\begin{aligned}((g_1,h_1)(g_2,h_2))(g_3,h_3) &= (g_1g_2, h_1h_2)(g_3,h_3)\\ &= ((g_1g_2)g_3, (h_1h_2)h_3)\\ &= (g_1(g_2g_3), h_1(h_2h_3))\\ &= (g_1,h_1)(g_2g_3, h_2h_3)\\ &= (g_1,h_1)((g_2,h_2)(g_3,h_3))\end{aligned}$$

(iii) Identity: If e_G and e_H are the identities of G and H then (e_G, e_H) is the identity of $G \oplus H$.
(iv) The inverse of (g,h) is (g^{-1}, h^{-1}) since everything takes place componentwise. ∎

This same construction process can be carried out with n groups where n is any positive integer. (In fact, it is even possible to do this with an infinite number of groups.) Given groups $G_1, \ldots, G_n$ we can create the direct product

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n = \{(g_1, g_2, \ldots, g_n) |\ g_i \in G_i\}.$$

Again the group operation is defined componentwise. For the most part we will concentrate on products of two groups.

EXAMPLE 0 Consider $\mathbf{Z}_4 \oplus \mathbf{Z}_6$. Find $|\mathbf{Z}_4 \oplus \mathbf{Z}_6|$. Determine $< (2,2) >$ and its order. Find $-(1,3)$. Are $(1,3)$ and $(3,1)$ in the same coset of $< 2,2 >$?

SOLUTION Since there are 4 choice for the first component and 6 for the second, Find $|\mathbf{Z}_4 \oplus \mathbf{Z}_6| = 24$. Next,

$$< (2,2) >= \{(0.0), (2,2), (0,4), (2,0), (0,2), (2,4)\}.$$

The inverse of $(1,3)$ is $(3,3)$. Now $(1,3)$ and $(3,1)$ are in the same coset of $< (2,2) >$ if and only if $-(1,3)+(3,1) = (3,3)+(3,1) = (2,4) \in < 2,2 >$. Yes.

EXAMPLE 1 Consider $U(9) \oplus \mathbf{Z}_9$. Find its order. Find $(2,2)^{-1}$. Find $< 4,6 >$. Are $(2,2)$ and $(3,3)$ in the same coset of $< 4,6 >$?

SOLUTION Since there are 6 choice for the first component and 9 for the second, Find $|\mathbf{Z}_4 \oplus \mathbf{Z}_6| = 54$. Next, $(2,2)^{-1} = (5,7)$ since $(2,2)(5,7) = (1,0)$.

$$< (4,6) >= \{(0.0), (4,6), (7,3), (1,0)\}.$$

Now $(2,2)$ and $(3,3)$ are in the same coset of $< (4,6) >$ if and only if $(2,2)^{-1}(3,3) = (5,7)(3,1) = (6,8) \in < (4,6) >$. No.

EXAMPLE

a) The most familiar example is if we let $G = H = (\mathbf{R}, +)$. Then $G \oplus H = \mathbf{R} \oplus \mathbf{R}$ which yields the addditive part of the ordinary vector space $\mathbf{R}^2$. By taking the product of n factors or copies of $\mathbf{R}$ we can obtain $(\mathbf{R}^n, +)$ the additive group of n-tuples of real numbers.

b) $\mathbf{Z}_2 \oplus S_3$. Its order is 12, the product of the number of elements in $\mathbf{Z}_2$ with the number of elemnents in D_3. What are these elements? □

LEMMA 1 *For any groups G and H,*

$$|G \oplus H| = \begin{cases} |G||H| & \text{if both } |G| \text{ and } |H| \text{ are finite.} \\ \infty & \text{otherwise.} \end{cases}$$

SOLUTION In the finite case, we have $|G|$ choices for the first component and $|H|$ choices for the second. Therefore

$$|G \oplus H| = |G||H|,$$

that is, the order of a product is the product of the orders. The infinite case is obvious. □

EXAMPLE 3 It is not the case that the product of cyclic groups is always cyclic. Consider $\mathbf{Z}_3 \oplus \mathbf{Z}_3$. If $(a, b) \in \mathbf{Z}_3 \oplus \mathbf{Z}_3$ then

$$(a, b) + (a, b) + (a, b) = (3a, 3b) = (0, 0) = e.$$

Of course this means that $|a, b| \mid 3$. But $|\mathbf{Z}_3 \oplus \mathbf{Z}_3| = 3 \cdot 3 = 9$, so no element of $\mathbf{Z}_3 \oplus \mathbf{Z}_3$ is a generator even though $\mathbf{Z}_3$ is cyclic.

LEMMA 2 *$G \oplus H$ is abelian if and only if G and H are both abelian.*

PROOF We have G and H abelian

$$\begin{aligned}
&\iff \begin{cases} g_1 g_2 = g_2 g_1 \ \forall g_1, g_2 \in G \\ h_1 h_2 = h_2 h_1 \ \forall h_1, h_2 \in H \end{cases} \\
&\iff (g_1 g_2, h_1 h_2) = (g_2 g_1, h_2 h_1) \ \forall g_1, g_2 \in G, \ \forall h_1, h_2 \in H \\
&\iff (g_1, h_1)(g_2, h_2) = (g_2, h_2)(g_1, h_1) \ \forall (g_1, h_1), (g_2, h_2) \ \forall \in G \oplus H \\
&\iff G \oplus H \text{ abelian}
\end{aligned}$$

EXAMPLE 4 $D_3 \oplus \mathbf{Z}_3$ is a non-abelian of order 18. So now you can construct lots of non-abelian groups by using products where one of the factors is D_n, S_n, Q_8, or $GL(n)$ where $n > 1$. For example, give me a non-abelian group of order 16.

Let's turn to the cyclic question. Notice that $(1, 1)$ in $\mathbf{Z}_2 \oplus \mathbf{Z}_3$ has order 6 (by direct observation). So $\mathbf{Z}_2 \oplus \mathbf{Z}_3$ is cyclic. But $\mathbf{Z}_3 \oplus \mathbf{Z}_3$ was not. Why? In the first case the powers of the individual generators did not interfere with one another while they did in the second case. What we need is a good way to compute the order of an element (g, h) of a product group via the orders of g and h.

THEOREM 3 *Let $g \in G$ and $h \in H$. If $|g|$ and $|h|$ are both finite, then $|(g, h)| = \text{lcm}(|g|, |h|)$ in $G \oplus H$.*

PROOF This proof is very similar in spirit to the proof that the order of a product of disjoint cycles in S_n was the lcm of their orders.

Let $m = |g|$ and $n = |h|$ and let $\text{lcm}(m, n) = L$. Then there are integers k, j so that $km = L$ and $jn = L$. Notice that

$$(g, h)^L = (g^L, h^L) = ((g^m)^k, (h^n)^j) = (e_G, e_H) = e,$$

so $|(g,h)| \mid L$. On the other hand if $|(g,h)| = p$, then $(g,h)^p = e$ so $(g^p, h^p) = (e_G, e_H)$ which means that $|g| \mid p$ and $|h| \mid p$. But L is the smallest integer that is divisible by both $|g|$ and $|h|$. Therefore $L \leq p$ so $|(g,h)| = L$. ∎

Example

a) Use the formula to check the orders of $(2,2)$ in $\mathbf{Z}_4 \oplus \mathbf{Z}_6$ and $(4,6)$ in $U(9) \oplus \mathbf{Z}_9$ that were calculated earlier.
Find the order of (5,6) in $\mathbf{Z}_6 \oplus \mathbf{Z}_{24}$. (Answer: 12)

b) Find the order of $(J, r_{30}) \in Q_8 \oplus D_{12}$. (Answer: 12)

Corollary 4 *Let G and H be cyclic groups of finite orders m and n. $G \oplus H$ is cyclic if and only if $(m,n) = 1$.*

PROOF Let $\gcd(m,n) = d$. Then $m = ad$ and $n = bd$ and we have seen that $\operatorname{lcm}(m,n) = abd$. Notice that $mn = abd^2$. So

$$mn = \operatorname{lcm}(m,n) \iff abd^2 = abd \iff d = 1 \iff \gcd(m,n) = 1.$$

Now let $G =< g >$ and $H =< h >$. Then $|g| = m$ and $|h| = n$ and $|G \oplus H| = mn$. So

$$|G \oplus H| = |(g,h)| \iff mn = \operatorname{lcm}(m,n) \iff \gcd(m,n) = 1. \ \square$$

Corollary 5 *Let $\mathbf{Z}_m \oplus \mathbf{Z}_n \cong \mathbf{Z}_{mn} \iff \gcd(m,n) = 1$.*

Example 6 What is the smallest value of n (greater than 1) that makes $\mathbf{Z}_{30} \oplus \mathbf{Z}_n$ cyclic?

Example 7 Show that $\mathbf{Z} \oplus \mathbf{Z}$ is **not** cyclic.

SOLUTION Assume that it is, and that it is generated by (m,n). Notice that $m \neq 0$, else all the multiples of $(m,n) = (0,n)$ would look like $(0,kn)$, which is clearly not all of $\mathbf{Z} \oplus \mathbf{Z}$. Similarly $n \neq 0$. Now $(1,0) \in \mathbf{Z} =< (m,n) >$ so there must be some $k \in \mathbf{Z}$ so that

$$k(m,n) = (1,0).$$

But then

$$(km, kn) = (1,0) \iff \begin{cases} km = 1 \\ kn = 0 \end{cases} \iff \begin{cases} k \neq 0 \\ k = 0 \end{cases} .$$

Contradiction ∎

Example 8 Of course product groups can have subgroups. For example in $\mathbf{Z} \oplus \mathbf{Z}$ we have such subgroups as $2\mathbf{Z} \oplus 3\mathbf{Z}$ (show this?) or $\{(k,k) |\ k \in \mathbf{Z}\}$. You can show that if A is a subgroup of G and B is a subgroup of H, then $A \oplus B$ is a subgroup of $G \oplus H$. But not all subgroups of products are products of subgroups as the example $\{(k,k) |\ k \in \mathbf{Z}\}$ shows.

1.2 Finite Abelian Groups

Much effort has been spent on classifying finite groups of all types (abelian and non-abelian). I strongly encourage you to read pages 355–357 in your text which profiles three living mathematicians who were crucial to solving a certain part of the classification problem.

The classification scheme for finite abelian groups has been known for a long time, and you are now in a position to understand it. Here's a simple example of the sort of problem that I am referring to. Suppose that $G = U(36)$, the group of units mod 36. With a bit of effort, you can show that $|U(36)| = 12$. Of course the group is abelian. Is it isomorphic to a more familiar group? It turns out to be isomorphic to $\mathbf{Z}_2 \oplus \mathbf{Z}_6$, which is a much "simpler" group to understand. How do I know that these groups are isomorphic? Well,...that takes some work.

The classification scheme for finite abelian groups uses the **Fundamental Theorem of Arithmetic**. Recall that any positiive integer $n \geq 2$ can be factored uniquely into a product of primes. For example

$$\begin{aligned} 200 &= 2^3 \cdot 5^2 \\ 48 &= 2^4 \cdot 3 \\ 300 &= 2^2 \cdot 3 \cdot 5^2 \end{aligned}$$

We'll see that there's a similar theorem that shows we can "factor" finite abelian groups into porducts of cyclic groups whose orders are powers of primes. Of course we know all about these latter groups.

There is one difference in the factorization process, however. Let's take 16 as an example. Using the Fundamental Theorem of Arithmetic, we would simply write

$$16 = 2^4.$$

However, when classifying abelian groups of order 16, we know that the following five groups are not isomorphic (why?):

$$\begin{aligned}
\mathbf{Z}_{16} &= \mathbf{Z}_{2^4} \\
\mathbf{Z}_8 \oplus \mathbf{Z}_2 &= \mathbf{Z}_{2^3} \oplus \mathbf{Z}_2 \\
\mathbf{Z}_4 \oplus \mathbf{Z}_4 &= \mathbf{Z}_{2^2} \oplus \mathbf{Z}_{2^2} \\
\mathbf{Z}_4 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 &= \mathbf{Z}_{2^2} \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \\
\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 &= \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2
\end{aligned}$$

It turns out that if G is abelian and its order is 16, then it must be isomorphic to one of the five groups listed above.

Notice that the list above has been arrived at in the most mechanical of ways. Since $16 = 2^4$, we have paritioned 4 into a sum of positive integers in as many ways as possible (disregarding order) on the right hand of each equality above. That is, $4 = 4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$. In a similar fashion we can find all possible partitions of 5.

$$5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1.$$

We are now ready to state:

THEOREM 6 ***(The Fundamental Theorem of Finite Abelian Groups)*** *Let G be a finite abelian group of order $|G| > 1$. Then G is isomorphic to the direct product of finitely many cyclic groups of prime power order. The prime powers that occur as orders of the factors are uniquely determined by G. In particular,*

$$G \cong \mathbf{Z}_{p_1^{n_1}} \oplus \mathbf{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbf{Z}_{p_k^{n_k}},$$

where the p's are primes such that $|G| = p_1^{n_1} \cdot p_2^{n_2} \cdots p_3^{n_3}$. Note the p_i need not be distinct primes.

PROOF The proof is quite long and in Chapter 12. For now I want to concentrate on how to use the theorem. ∎

EXAMPLE 9 What group is V_4, the Klein Four-Group? We know it is abelian and of order 4. Since $4 = 2^2 = 2^1 \cdot 2^1$, then by the Fundametal Theorem above, V_4 is either $\mathbf{Z}_{2^2} = \mathbf{Z}_4$ or $\mathbf{Z}_2 \oplus \mathbf{Z}_2$. But we know that $g^2 = e$ for all elements in V_4. So V_4 has no element of order 4. Therefore it cannot be cyclic. So V_4 is isomorphic to $\mathbf{Z}_2 \oplus \mathbf{Z}_2$.

EXAMPLE 10 Classify all abelian groups of order less than 20. I will get you started.

SOLUTION We will use the fundamental theorem above and the partitions of the factorizations of the various orders. First notice that if p is prime, then

an abelian group of prime order must be isomorphic to $\mathbf{Z}_p$. The Fundamental Theorem allows for no other possiblity. This takes care of abelian groups of orders: 2, 3, 5, 7, 11, 13, 17, 19

$$|G| = 4 = 2^2 = 2^1 \cdot 2^1 \Rightarrow G \cong \begin{cases} \mathbf{Z}_4 \\ \mathbf{Z}_2 \oplus \mathbf{Z}_2 \end{cases}$$

$$|G| = 6 = 2 \cdot 3 \Rightarrow G \cong \mathbf{Z}_2 \oplus \mathbf{Z}_3 \cong \mathbf{Z}_6$$

$$|G| = 8 = 2^3 = 2^2 \cdot 2^1 = 2 \cdot 2 \cdot 2 \Rightarrow G \cong \begin{cases} \mathbf{Z}_8 \\ \mathbf{Z}_4 \oplus \mathbf{Z}_2 \\ \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \end{cases}$$

$$|G| = 9 = 3^2 = 3^1 \cdot 3^1 \Rightarrow G \cong \begin{cases} \mathbf{Z}_9 \\ \mathbf{Z}_3 \oplus \mathbf{Z}_3 \end{cases}$$

$$|G| = 10 = 2 \cdot 5 \Rightarrow G \cong \mathbf{Z}_2 \oplus \mathbf{Z}_5 \cong \mathbf{Z}_{10}$$

$$|G| = 12 = 2^2 \cdot 3 = 2 \cdot 2 \cdot 3 \Rightarrow G \cong \begin{cases} \mathbf{Z}_4 \oplus \mathbf{Z}_3 \cong \mathbf{Z}_{12} \\ \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3 = \mathbf{Z}_2 \oplus \mathbf{Z}_6 \end{cases}$$

Fill in the rest up to order 20. ∎

Example 11 Let's return to the $U(36)$ example. Since it has 12 elements and is abelian, it is isomorphic to either $\mathbf{Z}_4 \oplus \mathbf{Z}_3$ or $\mathbf{Z}_2 \oplus \mathbf{Z}_6$. Now $\mathbf{Z}_4 \oplus \mathbf{Z}_3$ is cyclic and of order 12 so it is isomorphic to $\mathbf{Z}_{12}$. From `Marc's U(n)` program, $U(36)$ is not cyclic, so it must be isomorphic to $\mathbf{Z}_2 \oplus \mathbf{Z}_6$. (As a check: Note that $U(n)$ has six elements of order 6: 5, 7, 11, 23, 29, 31. So does $\mathbf{Z}_2 \oplus \mathbf{Z}_6$: (0,1), (0,5), (1,2), (1,4), and (1,6). Both have two elements of order 3: 13, 25 and (0,2), (0,4). Both have three elements of order 2: 17, 19, 35 and (0,3), (1,0), (1,3).

Example 12 Consider $U(180)$. It has 48 elements. BY FTFAG, it must be isomorphic to one of the following:

$$48 = 16 \cdot 3 \to \mathbf{Z}_{16} \oplus \mathbf{Z}_3 \cong \mathbf{Z}_{48}$$

$$48 = 2 \cdot 8 \cdot 3 \to \mathbf{Z}_2 \oplus \mathbf{Z}_8 \oplus \mathbf{Z}_3 \cong \mathbf{Z}_2 \oplus \mathbf{Z}_{24}$$

$$48 = 4 \cdot 4 \cdot 3 \to \mathbf{Z}_4 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_3 \cong \mathbf{Z}_4 \oplus \mathbf{Z}_{12}$$

$$48 = 2 \cdot 2 \cdot 4 \cdot 3 \to \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_3 \cong \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_{12} \cong \mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_6$$

$$48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \to \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3 \cong \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_6$$

Now `Marc's U(n)` gives the following data. There are no elements of order 12 or 24; 7 elements of order 2, 2 elements of order 3, 8 elements of order 4, 14 elements of order 6, and 16 elements of order 12. $U(180)$ cannot be with of the first two groups which have elements of order 24 and or 48. Similarly, it cannot be $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_6$ since this group has no elements of order 12. So let's look at $\mathbf{Z}_4 \oplus \mathbf{Z}_{12}$ and $\mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_6$. $\mathbf{Z}_4 \oplus \mathbf{Z}_{12}$

has 3 elements of order 2: (2,0), (2,6), and (0,6) while $\mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_6$ has has 7 elements of order 2: (0,0,3), (0,1,3), (1,0,3), (1,1,3), (0,1,0), (1,0,0), (1,1,0). So $U(180)$ must be this latter group.

Example 13 Write a Java version of `Marc's U(n)` program for massive extra credit.