Math 458: Notes on the classification of finite abelian groups

Given two groups $(G_1, *_1)$ and $(G_2, *_2)$, we can make a new group called $G_1 \times G_2$ as follows. As a set, $G_1 \times G_2 = \{(x, y) \mid x \in G_1, y \in G_2\}$. The group operation is given by

$$(x, y) * (a, b) = (x *_1 a, y *_2 b).$$

The group $G_1 \times G_2$ is called the **direct product** of G_1 and G_2. Note that if G_1 and G_2 are finite, with numbers of elements n_1 and n_2, then the size of $G_1 \times G_2$ is $n_1 n_2$.

The groups that we are the most familiar with are $\mathbb{Z}/n$, for various n. We now get a bunch more by looking at $\mathbb{Z}/k \times \mathbb{Z}/n$, $\mathbb{Z}/k \times \mathbb{Z}/l \times \mathbb{Z}/n$, and so forth. Sometimes these groups are secretly the same:

Example 1.1. The Chinese Remainder Theorem shows that if n and k are relatively prime then $\mathbb{Z}/n \times \mathbb{Z}/k \cong \mathbb{Z}/(nk)$. For example,

$$\mathbb{Z}/2 \times \mathbb{Z}/5 \cong \mathbb{Z}/10.$$

Example 1.2. The groups $G_1 \times G_2$ and $G_2 \times G_1$ are isomorphic, via the function that sends (x, y) to (y, x). For this reason we are often cavalier about the order we write factors in a direct product. For example, $\mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/8$ and $\mathbb{Z}/8 \times \mathbb{Z}/2 \times \mathbb{Z}/4$ are isomorphic groups.

Example 1.3. The groups $\mathbb{Z}/2 \times \mathbb{Z}/2$ and $\mathbb{Z}/4$ are both abelian groups of order 4. Are they isomorphic? The group $\mathbb{Z}/2$ has the property that $x + x = 0$ for every x, and so if $(x, y) \in \mathbb{Z}/2 \times \mathbb{Z}/2$ then

$$(x, y) + (x, y) = (x + x, y + y) = (0, 0).$$

So every element of $\mathbb{Z}/2 \times \mathbb{Z}/2$, when added to itself, gives the identity element. But this is NOT true of $\mathbb{Z}/4$: $1 + 1 \neq 0$ here. This difference shows that the two groups $\mathbb{Z}/2 \times \mathbb{Z}/2$ and $\mathbb{Z}/4$ are not isomorphic.

Similar reasoning can be used to show that when n and k are NOT relatively prime then $\mathbb{Z}/n \times \mathbb{Z}/k \ncong \mathbb{Z}/(nk)$.

The following is an important theorem in basic group theory. We will not explain the proof here (it is covered in many introductory courses on abstract algebra), but we will use the result often.

Theorem 1.4 (Classification of finite abelian groups)**.** *Let A be a finite abelian group whose number of elements is n. Then A is isomorphic to exactly one group of the form*

$$\mathbb{Z}/p_1^{e_1} \times \mathbb{Z}/p_2^{e_2} \times \cdots \times \mathbb{Z}/p_k^{e_k}$$

(up to permutation of the factors) where the p_i are primes (not necessarily distinct) and $n = p_1^{e_1} \cdots p_k^{e_k}$.

Example 1.5. We can use the theorem to write down all abelian groups of order 8. Since the only prime dividing 8 is 2, the factors will all have to be powers of 2. So the possibilities are

$$\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2, \quad \mathbb{Z}/2 \times \mathbb{Z}/4, \quad \text{and} \quad \mathbb{Z}/8.$$

These are the only ways to select powers of 2 whose product gives us 8.

Example 1.6. Next let's use the theorem to write down all abelian groups of order 200. We factor $200 = 2^3 \times 5^2$, then we handle the different primes separately. The classification theorem says that our group will decompose as

$$(\text{abelian group of order } 2^3) \times (\text{abelian group of order } 5^2)$$

and we found all the possibilities for the first factor in the previous example. For the second factor, the possibilities will be

$$\mathbb{Z}/5 \times \mathbb{Z}/5 \quad \text{and} \quad \mathbb{Z}/25.$$

So altogether we get $3 \cdot 2 = 6$ possible groups:

- $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/5 \times \mathbb{Z}/5$
- $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/25$
- $\mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/5 \times \mathbb{Z}/5$
- $\mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/25$
- $\mathbb{Z}/8 \times \mathbb{Z}/5 \times \mathbb{Z}/5$
- $\mathbb{Z}/8 \times \mathbb{Z}/25$

We can use the Chinse Remainder Theorem to simplify how we write some of these groups, by combining relatively-prime pieces into one as follows:

- $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/5 \times \mathbb{Z}/5 \cong \mathbb{Z}/2 \times \mathbb{Z}/10 \times \mathbb{Z}/10$
- $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/25 \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/50$
- $\mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/5 \times \mathbb{Z}/5 \cong \mathbb{Z}/20 \times \mathbb{Z}/10$
- $\mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/25 \cong \mathbb{Z}/2 \times \mathbb{Z}/100 \cong \mathbb{Z}/4 \times \mathbb{Z}/50$
- $\mathbb{Z}/8 \times \mathbb{Z}/5 \times \mathbb{Z}/5 \cong \mathbb{Z}/40 \times \mathbb{Z}/5$
- $\mathbb{Z}/8 \times \mathbb{Z}/25 \cong \mathbb{Z}/200$

We can distinguish groups on our list by considering the orders of different elements. Recall that if A is an abelian group and $a \in A$, then the **order** of a is the smallest positive integer n such that $na = 0$. Here na means $a + a + \cdots + a$ (n times).

Example 1.7. The order of 0 is always 1, since $1 \cdot 0 = 0$.

Example 1.8. In $(\mathbb{Z}/N, +)$, the order of 1 is N. If $a \in \mathbb{Z}/N$ is any element, its order divides N. To see this, consider the sequence

$$0, a, 2a, 3a, 4a, \ldots, Na, (N+1)a, \ldots$$

We know $Na = 0$ in $\mathbb{Z}/N$, so the order of a is at most N. But it could be smaller: for example, in $\mathbb{Z}/6$ we have $2 + 2 + 2 = 0$ and the order of 2 is 3. If k denotes the order of our element a, then the above sequence first becomes 0 at the kth step. But that means it is next 0 at the $(2k)$th step, and then at the $(3k)$th step, and so forth. So we know the sequence becomes 0 only at these multiples of k, but we ALSO know it becomes 0 at step N. So N is a multiple of k (or equivalently, k divides N).

Now let A and B be two abelian groups, let $a \in A$, and $b \in B$. Let k be the order of a, and let l be the order of b. What is the order of (a, b) in $A \times B$? If we think about the sequence

$$(0,0), (a,b), (2a, 2b), (3a, 3b), \ldots$$

we see that the first coordinate becomes 0 every k steps, and the second coordinate becomes 0 every l steps. So both coordinates becomes 0 at once every $\text{lcm}(k, l)$ steps. This proves the following useful fact:

$$\boxed{\text{order}((a,b)) = \text{lcm}(\text{order}(a), \text{order}(b))}$$

We can use this to prove that certain groups are not isomorphic. For example, in $\mathbb{Z}/4$ the largest order of any element is 4 and in $\mathbb{Z}/2$ the largest order of any element is 2. So in $\mathbb{Z}/4 \times \mathbb{Z}/2$ the largest order possible is $\text{lcm}(4, 2) = 4$. In contrast, we know that in $\mathbb{Z}/8$ the largest order of any element is 8; so this proves that these two groups are different:

$$\mathbb{Z}/4 \times \mathbb{Z}/2 \ncong \mathbb{Z}/8.$$

This technique of "looking at the largest order possible" works to prove that many abelian groups are not isomorphic, but it has its limits. For example, the largest order of an element in $\mathbb{Z}/4 \times \mathbb{Z}/4$ is $\text{lcm}(4, 4) = 4$, and the largest order of an element in $\mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/2$ is $\text{lcm}(4, 2, 2) = 4$. But these groups are still not isomorphic. To see why, let's do a deeper dive into the orders of the elements. The table on the left shows the orders for elements in $\mathbb{Z}/4 \times \mathbb{Z}/4$, and the one on the left shows the orders for elements in $\mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/2$:

element	order
(0,0)	1
(0,1)	4
(0,2)	2
(0,3)	4
(1,0)	4
(1,1)	4
(1,2)	4
(1,3)	4
(2,0)	2
(2,1)	4
(2,2)	2
(2,3)	4
(3,0)	4
(3,1)	4
(3,2)	4
(3,3)	4

element	order
(0,0,0)	1
(0,0,1)	2
(0,1,0)	2
(0,1,1)	2
(1,0,0)	4
(1,0,1)	4
(1,1,0)	4
(1,1,1)	4
(2,0,0)	2
(2,0,1)	2
(2,1,0)	2
(2,1,1)	2
(3,0,0)	4
(3,0,1)	4
(3,1,0)	4
(3,1,1)	4

Note that we got these tables just by using the lcm rule for orders, and the fact that we can easily compute orders in $\mathbb{Z}/N$.

For $\mathbb{Z}/4 \times \mathbb{Z}/4$, we only have three elements of order 2 and twelve elements of order 4. In $\mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/2$ we have seven elements of order 2 and eight elements of order 4. So these groups are not isomorphic.

For finite abelian groups, this kind of analysis always works. If two such groups are not isomorphic, you will always be able to see that by analyzing the numbers of elements with different orders, as we have done here.