Math 222: Classifying Finite Groups

One of the primary problems in group theory has been (and in some sense still is) the classification of all finite groups – i.e. What are all the finite groups? Let's explore this question a little. In class we have already seen one nice fact:

Theorem 1. If G is a finite group of order a prime number p, then G is cyclic and isomorphic to $\mathbb{Z}_p$.

Note: For convenience, we'll simply denote the group of integers mod n under addition, $(\mathbb{Z}_n, +)$, by $\mathbb{Z}_n$.

This theorem followed from one of the most important results of group theory:

Lagrange's Theorem. If H is a subgroup of a finite group G, then the order of H divides the order of G.

Another fundamental result is

Cauchy's Theorem. (Theorem 11.8) If the order of a finite group G is divisible by a prime p, then G has an element of order p.

This allows one to tackle groups of order $2p$ with $p > 2$. By Cauchy's Theorem there exists an element $a \in G$ with order p and an element $b \in G$ with order 2. The cyclic subgroup $\langle a \rangle$ has order p and so has index 2 in G. Hence, this is normal. Using normality and considering the element bab^{-1}, one can show the following:

Theorem 2. (Corollary 11.9) If $p > 2$ and G is a finite group of order $2p$, then G is isomorphic to either $\mathbb{Z}_p$ or D_p.

Example 1. Hence, there are only two groups of order $6 = 2 \cdot 3$: $\mathbb{Z}_6$ and $D_3 \simeq S_3$. And there are only two groups of order $10 = 2 \cdot 5$: $\mathbb{Z}_{10}$ and D_5.

Let's now consider abelian groups. There is a beautiful description of what all the finite abelian groups are. To state this we need to the notion of the product of two groups – see section 11.1. This is an easy way to build new groups from old. Suppose we have two groups G and H. Then we get a new group $G \times H$ which is simply the set of all ordered pairs

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

with "componentwise" multiplication. That is $(a, b) \cdot (c, d) = (a \cdot c, b \cdot d)$ where the multiplication on the left is in G and the multiplication on the right is in H.

Example 2. Consider the group

$$G = \mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}.$$

For example $(0, 1) + (1, 1) = (1, 2)$, $(0, 1) + (1, 2) = (1, 3)$, $(0, 2) + (0, 2) = (0, 1)$, and so on. The identity element here is of course $(0, 0)$. This group has order 6 and so by Theorem 2 it must be isomorphic to either $\mathbb{Z}_6$ or D_3. But, it's clearly abelian and so couldn't be the latter. Indeed, notice that the element $(1, 1)$ has order 6 and so G is indeed cyclic with $G = \langle (1, 1) \rangle$.

Example 2.1 Consider now the group

$$G' = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}.$$

Now, this group has order 4 and in analogy with the previous example you might guess that G' is ismorphic to $\mathbb{Z}_4$. But, being clever you quickly notice that each non-identity element in G' has order TWO! So, it's in fact the Klein Four group. Hmm.... what's going on here?

Question: What's different in these two situations?

In the first case, we're dealing with two different primes – 2 and 3, whereas in the second case, we're dealing with the same prime – 2. Indeed, the starting point for identifying all finite abelian groups are the following two facts.

Theorem 3. Let p, q be distint prime numbers. The group $\mathbb{Z}_p \times \mathbb{Z}_q$ is cyclic and isomorphic to $\mathbb{Z}_{pq}$. More generally, the statement holds for any integers p and q which are relatively prime.

Proof. Can you prove this?

Theorem 4. Let p be prime. The group $\mathbb{Z}_p \times \mathbb{Z}_p$ is NOT cyclic and hence not isomorphic to the group $\mathbb{Z}_{p^2}$.

Proof. Can you prove this? Consider order. Is there a more general statement?

Example 3. If we consider groups of order $9 = 3 \cdot 3$, just like for order 4, we get two distinct abelian groups: $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Example 3.1. But, compare this to order $8 = 2 \cdot 2 \cdot 2$. We can build up several potentially different abelian groups:

$$\mathbb{Z}_8, \quad \mathbb{Z}_4 \times \mathbb{Z}_2, \quad \text{and} \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Are any of these the same? No. Consider the order of elements. The latter two have no elements of order 8 and so cannot be $\mathbb{Z}_8$. Similarly, the last one has no elements of order 4 and so must be distinct from both the first and second group.

In the examples above, we see that when one is dealing with a product of distinct prime numbers, there are not so many options, but when dealing with a power of a prime there are many options. What then is true in general? The following beautiful result:

Fundamental Theorem of Finite Abelian Groups. Every finite abelian group is isomorphic to a product of the form

$$\mathbb{Z}_{p_1}^{n_1} \times \mathbb{Z}_{p_2}^{n_2} \times \cdots \times \mathbb{Z}_{p_k}^{n_k}$$

for some collection of not necessarily distinct primes p_i and positive integers n_i. Moreover, this factorization is unique except for rearrangement of the factors.

Example 4. What are all the abelian groups of order 120? To answer this, we first factor 120 into a product of primes: $120 = 2^3 \cdot 3 \cdot 5$. For each distinct prime (or power thereof) we consider all the possible abelian groups of that order:

- $8 = 2^3$: $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
- 3: $\mathbb{Z}_3$
- 5: $\mathbb{Z}_5$

Now, the possible groups of order 120 consists of products of groups – exactly one coming from each of the three lists. So, here there are three possible groups:

- $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{120} \simeq \mathbb{Z}_{24} \times \mathbb{Z}_5 \simeq \mathbb{Z}_8 \times \mathbb{Z}_5$
- $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_4 \times \mathbb{Z}_{30} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{60}$

- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

Example 4.1: The finite abelian groups of order $108 = 3^3 \cdot 2^2$ are

- $\mathbb{Z}_{27} \times \mathbb{Z}_4 \simeq \mathbb{Z}_{108}$
- $\mathbb{Z}_{27} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \simeq \mathbb{Z}_{54} \times \mathbb{Z}_2$
- $\mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \simeq \mathbb{Z}_9 \times \mathbb{Z}_{12} \simeq \mathbb{Z}_3 \times \mathbb{Z}_{36}$
- $\mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \simeq \mathbb{Z}_9 \times \mathbb{Z}_6 \times \mathbb{Z}_2$
- $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_4$
- $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Problems: Find all the finite abelian groups of order: 64, 212, 600, 1000, and 1250.

While the classification of finite abelian groups dates back to the 1800's a more recent and monumental project has been the classification of finite *simple* groups. Recall that a group is simple if it has no non-trivial normal subgroups. For example, for any prime p, the cyclic group $\mathbb{Z}_p$ is simple because it has no non-trivial subgroups period. And from our above discsussion we see that those are the only abelian simple groups. How about non-abelian ones? We have also seen that the alternating group A_5 is simple – indeed for each $n > 4$, A_n is simple.

The project of classifying all the simple groups began in the early 60's (late 50's perhaps) with a monumental theorem by Feit and Thompson which says that any non-abelian simple group must have even order. Throughout the 60's and 70's there was an amazing collaborative effort among Group Theorists to solve this problem ... the problem was divied up into chunks and worked on by various mathematicians. After some 10,000+ pages of published material and 20-25 years of effort, the problem was solved! There are 18 infinite families of finite simple groups – we have noted the first two of these above. And then there are 26 other, so called "sporadic" groups, which don't seem to fit with anything. And that's it!

As a further testament to the enormity of the project, lest you think you might stumble upon these simple groups ... the largest of the sporadic groups, called the "Monster" group has order ... hold onto your socks! ...

$$808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000.$$

That's more than the number of atoms in the earth! Only a mathematician could call such a group simple.

As well as being a wonderful example of the power of collaboration, this project showed that even mathematicians have a few skeletons in their closets. Because of the scattered nature of the original proofs of this, two mathematicians are writing a series of books containing a complete proof. (I believe volume 3 or 4 of a predicted 10 has just come out.) In the process it has been discovered that things are not in fact fully complete. One mathematician whose task it was to prove some piece of the puzzle never published his work and so others have had to come along and fill in some gaps in his work.