Finite group

So far, we have met the dihedral group D_4, the cyclic group C_n, the symmetric group $\mathcal{S}_n$, and the alternating group $\mathcal{A}_n$. We have seen that D_4 had 8 elements, C_n had n elements, $\mathcal{S}_n$ had $n!$ elements, and $\mathcal{A}_n$ had $n!/2$ elements. The number of elements of group is called "order," and is often denoted by $||$. For example,

$$|D_4| = 8, \qquad |C_n| = n, \qquad |\mathcal{S}_n| = n!, \qquad |\mathcal{A}_n| = n!/2 \tag{1}$$

Notice that the order of these groups are finite. In other words, not infinite. A group whose order is finite is called "finite group." Then, one may wonder, whether it would be possible to classify *all* finite groups. We are curious to know what are the all possible finite groups.

How do we do this? Well, let's start with group with order 1. Apparently, this group is e where e is the identiy element. It has an inverse, which is $e^{-1} = e$. Now, let's move on to group with order 2. Of the two elements of this group, one must be the identity element, and another must be an element that is *not* the identity element. Otherwise, there is only one element, namely, the identity element in the group, which would mean that the order of this group is 1. Let's call the other element by a. Then, its inverse a^{-1} must be either e or a, but e doesn't make sense, because we want

$$a^{-1} \bullet a = a \bullet a^{-1} = e \tag{2}$$

where as e satisfies

$$e \bullet a = a \bullet e = a \tag{3}$$

Thus, we conclude that $a^{-1} = a$. In other words,

$$a \bullet a = e \tag{4}$$

So, we obtained all the group multiplication rules for this group. We have

$$e \bullet e = e, \quad a \bullet e = e \bullet a = a, \quad a \bullet a = e \tag{5}$$

Thus, we see that the group which satisfies the above group multiplication rule is the only group that has order 2.

We may continue this way. We can exhaust all the possibilities for multiplication rules for group with order 3. It is not hard to prove that the only consistent multiplication rule for group with order 3 is given by

$$e \bullet e = e, \qquad e \bullet a = a, \qquad e \bullet b = b \tag{6}$$

$$a \bullet e = a, \qquad a \bullet a = b, \qquad a \bullet b = e \tag{7}$$

$$b \bullet e = b, \qquad b \bullet a = e, \qquad b \bullet b = a \tag{8}$$

where we denoted the element of this group by $\{e, a, b\}$.

Problem 1. Convince yourself that this is the only possibility for group with order 3. (Hint[1])

Problem 2. Is this group Abelian?

Actually, careful reader may have noticed that this is the exactly same group as C_3, upon the following identification:

$$e \to \bar{0}_3, \qquad a \to \bar{1}_3, \qquad b \to \bar{2}_3 \tag{9}$$

So, one may move onto groups with order 4, groups with order 5, and so on. It turns out that there are two groups with order 4, one group with order 5, two groups with order 6, one group with order 7, 10 groups with order 8, and so on.

But, we will never reach the end by such a method. There will be infinitely many groups to analyze.

Luckily, mathematicians worked very hard to classify all groups using a lot of techniques. They found out that groups can either be decomposed into smaller groups, or can't. I cannot explain what this decomposition is as it is beyond the scope of this article, but it is similar to the way how a number can either be decomposed into a product of two smaller numbers or can't. In the first case, the number is not a prime. For example, $12 = 3 \times 4$, and 12 is not a prime. In the second case, the number is a prime. For example, $7 = 7 \times 1$, but 7 on the right-hand side is not smaller than 7 on the left-hand side. 7 is a prime. Once you decompose a number into a product of smaller numbers, you can decompose smaller numbers into a product of even smaller numbers again. For example, we had $12 = 3 \times 4$, and 4 can be expressed as $4 = 2 \times 2$. By continuing this way, you finally reach full decomposition. In case of number, a number can be expressed as a product of primes. Similar process can be done for a group. It can be expressed as a "product" of groups that are called "semi-simple group."[2] Again, I cannot exactly tell what "product" or "semi-simple group" means, but you may regard

[1] Why can't $a \bullet b$ be a or b? Then, what must $a \bullet b$ be? Similarly, figure out what $b \bullet a$ must be.

[2] The actual precise mathematical terminology here is not "product," but I just used this terminology to ease your understanding.

semi-simple group as "prime" of groups. Thus, to classify all groups, all we need to do is classifying semi-simple groups.

Luckily, mathematicians classified all semi-simple groups. The classification theorem of semi-simple groups says that every finite semi-simple group is one of the following groups:

- the cyclic groups of prime order (i.e., $C_2, C_3, C_5, C_7, C_{11}, \cdots$)
- the alternating group of degree at least 5 (i.e., $\mathcal{A}_5, \mathcal{A}_6, \mathcal{A}_7, \cdots$)
- the groups of Lie type
- one of 26 groups called the "sporadic group"
- the Tits group (sometimes considered as the 27th sporadic group)

This theorem was proven together by about hundred mathematicians mainly from 1955 to 2004. The proof consists of tens of thousands of page in several hundred papers. The final proof was done by Ashbacher and Smith in 1221-page paper. Now, mathematicians are working hard to simplify the proof, and summarize it, so that posterity can read it.

In our essay "Surprises in math, the reason why I study physics, and a recommendation for "The Number Devil"," we briefly mentioned the Monster group. The Monster group is the biggest sporadic group, which has the order

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

Summary

- The number of elements of a group is called "order."
- The group with finite order is called "finite group."
- The finite group is completely classified.