Math Circles. Group Theory. Session 3.

Diana Carolina Castañeda Santos
dccastan@uwaterloo.ca
University of Waterloo

April 3, 2019

1 Properties of Groups and isomorphic groups

Proposition: (Cancellation) Let G be a group and let $a, b, c \in G$. If $ac = bc$, then $a = b$.

Proof. Since G is a group, we know that the inverse of c, namely c^{-1} exists, so we can multiply by the right by c^{-1} and obtain

$$\begin{aligned} ac &= bc \\ (ac)(c^{-1}) &= (bc)(c^{-1}) \\ a(cc^{-1}) &= b(cc^{-1}) \\ a(e) &= b(e) \\ a &= b \end{aligned}$$

The third line is possible because of the property of associativity in G. The fourth line is due to the property of inverses in G and the last line is possible because of the property of the identity in G. This completes the proof. □

So far we have seen examples of groups and some properties of them. But one important aspect of studying groups is to determine how many of them actually exist. Do we have groups of any order? More specifically, given a natural number n, can we find groups of order n? How many distinct groups of that order exist?

What do you think? Discuss with a partner: Given a natural number n, can we find groups of order n?

_____.

Let's start studying this question by studying the number of elements in a group.

Can we have a group with one element? _____.

_____.

Now, let's study groups with two elements. Say that we want a group with elements $\{e, a\}$. Let's check out the multiplication table. We know how to operate with the identity element. Also remember that any element shows up in each column and each row exactly once. So the table is:

$\cdot$	e	a
e	e	a
a	a	

Well, this table is very familiar, we already know two groups with two elements. $(\mathbb{Z}_2, +)$ and $(\mathbb{Z}_4^*, \cdot)$. These two groups have different elements but their tables are the same. so if we care only about the structure, we say that these two groups are the same group. So there is only one group of order 2.

Let's study groups of order 3. Say that we have a group with three elements $\{e, a, b\}$. As before we try to complete the multiplication table. To do it, we use the properties of the identity element and the fact that we can't repeat elements in columns or rows. The table is given by:

$\cdot$	e	a	b
e	e	a	b
a	a		
b	b		

Notice that as before, we only have one possible way to complete this table, so if we care only about the structure, there is only one group of order 3. In fact we know a group like this one $(\mathbb{Z}_3, +)$.

In the process of studying groups of order n for each $n \in \mathbb{N}$, the following definition became more clear. We were trying to say that two groups are the same if we look at

their multiplication table and it looks pretty much the same up to relabel the elements.

Definition: Two groups are said to be **isomorphic** if one can relabel the elements of one group with the elements of the other in such a way that after relabel and reorder the multiplication tables are the same.

Examples:

- $(\mathbb{Z}_2, +)$ and $(\mathbb{Z}_6^*, \cdot)$ are isomorphic.

- $(\mathbb{Z}_8^*, \cdot)$ isomorphic to $(\{1, -1, i, -i\}, \cdot)$

2 Subgroups

Remember that one of the exercises for the first session was to prove that $(2\mathbb{Z}, +)$ is a group. Also, the problem asked to relate this group with $(\mathbb{Z}, +)$, and we noticed that $2\mathbb{Z}$ is contained in $\mathbb{Z}$ with the same operation "+". SO let's formalize this notion, by defining what a subgroup is.

Definition: Let $(G, *)$ be a group. A subgroup of G is a subset A such that $(A, *)$ is a group by itself. We denote this by $A \leq G$

Examples:

1. Any group G has at least two subgroups, $\{e\}$ and G itself. These are called the trivial subgroups of G.
2. $\{0, 2\}$ is a subgroup of $\mathbb{Z}_4$.
3. $\{e, H\}$, $\{e, R, R^2, R^3\}$ are subgroups of D_4.
4. S_3 is a subgroup of S_4 and moreover for all n, $S_n \leq S_{n+1}$.

Let's study the subgroups of $\mathbb{Z}_6$ (Remember that we really mean $(\mathbb{Z}_6, +)$). Well, first we find the two trivial subgroups which are $\{0\}$ and $\mathbb{Z}_6$. Now, say that a subgroup contains 0 and 1, then $1 + 1$ will be there, $1 + 1 + 1$, $1 + 1 + 1 + 1$ will be there too, and so on. so , if a group contains 1, it has to be $\mathbb{Z}_6$.

How about a subgroup containing 0 and 2? _____

How about a subgroup containing 0 and 3? _____

How about a subgroup containing 0 and 4? _____

How about a subgroup containing 0 and 5? _____

Great! We have found all the subgroups of $\mathbb{Z}_6$, which are _____

_____

Theorem: Let $(G, *)$ be a group. Let H be a subset of G that is not empty. H is a subgroup of G if it satisfies the following two conditions:

1. For all $a, b \in H$, $a * b \in H$.
2. For all $a \in H$, $a^{-1} \in H$.

Proof. We need to verify the four conditions to be a group on H.

- **The operation $*$ is closed:** This follows because of the first property.
- **Associativity:** This says that if a, b, c are in H then $(a * b) * c = a * (b * c)$. But since H is a subset of G, associativity holds in G so this is true in H.
- **Identity:** Prove that H has an identity element.
- **Inverses:** This property is precisely the second property.

□

In our previous example of finding the subgroups of $\mathbb{Z}_6$, notice that we got subgroups of order 1, 2, 3 and 6. It seems a coincidence that actually these are divisors of 6 the order of the group $\mathbb{Z}_6$. In fact, let's look at more examples:

Let G denotes a group and H denotes a subgroup of G.

G	H	$\lvert G\rvert$	$\lvert H\rvert$
$\mathbb{Z}_8$	$\{0, 2, 4, 6\}$	8	4
$\mathbb{Z}_{11}^*$	$\{1, 3, 4, 5, 9\}$	10	5
D_4	$\{e, V\}$	8	2
D_4	$\{e, R, R^2, R^3\}$	8	4
S_4	S_3	24	6

Well, this is actually not a coincidence. This is a very important property that groups have. This property was found by the mathematician Joseph-Louis Lagrange.

Theorem: (Lagrange) Let G be a finite group and let H be a subgroup of G, then $|H|$ divides $|G|$.

Proof. Let $H = \{h_1, h_2, \cdots, h_k\}$. For each element $a \in G$ we construct the set $aH = \{ah_1, ah_2, \cdots, ah_k\}$ which we call it a *coset*. Notice that for each $a \in G$ the set aH is a subset of G. The idea of the proof is to realize that these sets cover all the set G and that the sizes of these sets add up to the size of G. Let's check some properties about these subsets of G.

1. **Any element in G belongs to some coset:** Well, recall that H is a group, in particular, the identity element e belongs to H, so for each element $a \in G$, $a = ae \in aH$.

   ♣♣ (This tells us that G is contained in the union of all those sets.)

2. **All cosets have the same size:** We need to be sure that $aH = \{ah_1, ah_2, \cdots, ah_k\}$ has exactly k elements. Assume that there are two elements ah_1 and ah_2 in aH that are equal. Remember that G is a group. Then $a^{-1} \in G$. So we can use the cancellation property in $ah_1 = ah_2$, hence $h_1 = h_2$.

   ♣♣ (This shows that all cosets have k elements.)

3. **Two cosets are disjoint or are equal:** Let aH and bH be two cosets, assume that they are disjoint. So, there is an element that belongs to both aH and bH. That element is of the form $ah_1 = bh_2$ for some $h_1, h_2 \in H$.

   Now, let $ah \in aH$ be an arbitrary element in the coset aH. Then

   $$ah = a(e)h = a(h_1h_1^{-1})h = b(h_2h_1^{-1}h)$$

   But since H is a group $h_2h_1^{-1}h$ is an element in H, so $ah = bh \in bH$. Similarly, we can prove that any element in bH is also an element in aH. Thus $aH = bH$.

   ♣♣ (This tells us that G is divided into sets all disjoint and with the same number of elements.)

   We are ready to finish the proof. Let $t = \#of disjoint cosets$, Since all cosets have the same size as the size of H, we conclude that $|G| = t|H|$. In other words $|H|$ divides the order of $|G|$.

□