A Brief Introduction to Group Theory

Introduction

The group theory has long been a fascinating cornerstone of abstract algebra. Although it might not yet have appeared in our textbooks, but it provides a fundamental framework for the understanding of symmetry, algebraic structures, and invariance. Moreover, it has numerous real-life applications in fields like cryptography, chemistry, physics, and computer science.[1]

One of the most inconspicuous applications of group theory is finding the formula of the roots for polynomial equations. You might have noticed that our calculators can only find roots for polynomials with degrees up to 4. This is not because they do not have enough capacity to do a complicated operation but is in fact due to the restriction of a theorem in group theory – Galois Theory. (However, we might figure out an approach to finding general formulas for polynomials with a higher degree one day. Who knows!)

Interested? Why not have a look at this fresh and handy concept?

Definition and Axioms

To get started, it shall be useful to break this huge, intimidating theory into pieces. Let's talk about groups first. Have you ever heard about groups?

If not, what about sets?

Sets are basically a collection of distinct random elements with no requirements on the order (total number of elements) or types of elements. The elements could be our most used numbers, letters from the alphabet, or even meaningless shapes and symbols, as long as all the elements are in the same category. Here are a few examples of sets:

$$\{4, 7, 38, 71\}$$

$$\{m, e, i, x, o, q, d, k, q, u\}$$

$$\{!, /, =, \$, \wedge, *\}$$

Groups, which we denote as G, are in fact quite similar to the sets, just with a few

[1] https://www.studysmarter.co.uk/explanations/math/decision-maths/group-theory-terminology/

more restrictions based on the rules of sets:

1. Each group involves one binary operation.
2. Each group contains one identity element.
3. All the elements within the group have one inverse.
4. All the groups have the property of closure.
5. All the groups have the property of associativity.

They might seem confusing at first glance, but don't worry, we'll explain them one by one.

Binary operations are simply operations between two elements like $+$, $\cdot$ and any other binary operations which we will write as $*$. The reason we don't mention $-$ or $\div$ here is that $1-1$ can be expressed as $1+(-1)$ while $4\div 2$ can be expressed as $4\times\frac{1}{2}$. Binary operations are essential for groups, and you have to write a group as $(G,*)$, where $*$ is our binary operation for the groups.

On the bases of that, all the groups contain an element, e, that would not change the other elements after the operation. For instance, in $(G,+)$, the identity element e shall be 0, since all the numbers remain the same when they plus 0 ($3+0=3$); whereas the e for $(G,\cdot)$ shall be 1, since all the numbers remain the same when they time 1 ($5\cdot 1=5$). The identity element can also be considered as an original form (starting point of transformation) of the other elements in the group, as all other elements can be obtained from e through binary operations. (i.e. $ae=a=ea$ for all $a,e\in G$)

Another crucial property of groups is that every element in the group has an inverse element, meaning the product obtained from the binary operation of element a and its inverse a^{-1} will be the identity element e. For example, in $(G,+)$, the inverse of 4 will be -4, since $4+(-4)=0$, and 0 is the identity element. (i.e. For all $a\in G$, there exists $b\in G$, such that $ab=e=ba$, and we denote b as a^{-1})

Furthermore, when elements a and b are contained in a group, their product through binary operation $a*b$ should also be in the group. To give an example, in $(G,+)$, if 1 and 2 are both included in G, then 3 (which is just $1+2$) should also be included in G. As all the elements and their products are within the group, the group formed is closed, thus this property is called closure.

Finally, just like $(1+2)+3=1+(2+3)$, the groups also follow an associative rule, so that in a chain operation (like the example above), which operation comes first will not affect the result. (i.e. $(ab)c=a(bc)$ for all $a,b,c\in G$) However, even though the

order of operation does not matter, the order of the elements does make an impact on the results (e.g. $M_1 \cdot M_2 \neq M_2 \cdot M_1$, where M_1 and M_2 are both matrices).

All the sets satisfying the above conditions are groups, and that leads us to a basic context of this theory, also summaries by Wikipedia as: [2]

A group is a non-empty set G together with a binary operation on G, denoted " $\cdot$ ", that combines any two elements $\mathbf{a}$ and $\mathbf{b}$ of $\mathbf{G}$ to form an element of $\mathbf{G}$, denoted $\mathbf{a} \cdot \mathbf{b}$, such that the following three requirements, known as group axioms, are satisfied:

Identity element
Inverse element
Associativity

We can now find the following group properties based on the above axioms using some rigorous and elegant proofs.

- **Property 1: In any group, identity element is unique.**

  Suppose there are two distinct identity elements e and e' in a group G,

  According to the property of identity element,

  $g \cdot e = e \cdot g = g$ for all $g \in G$

  $g \cdot e' = e' \cdot g = g$ for all $g \in G$

  Since $e, e' \in G$,

  $e' \cdot e = e \cdot e' = e'$ and $e \cdot e' = e' \cdot e = e$ both hold

  $\therefore e = e'$

  This contradicts the fact that there are two distinct identity elements e and e' in G

  Therefore, there is only one unique identity element in any group.

- **Property 2: In any group, each element has one unique inverse element.**

  Suppose there are two distinct inverse elements a and b for one element g in a group G,

  According to the property of inverse element,

  $a = a \cdot e$

  $a = a \cdot (g \cdot b)$

  $a = (a \cdot g) \cdot b$ (due to the property of associativity)

  $a = e \cdot b$

  $\therefore a = b$

  This contradicts the fact that there are two distinct inverse elements a and b for

[2] https://en.wikipedia.org/wiki/Group_(mathematics)#Definition_and_illustration

g in G

Therefore, there is only one unique inverse element for each element in any group.

- **Property 3: In any group, the element is itself the inverse element of its inverse.**

  Suppose there are two distinct elements g and its inverse g^{-1} in a group G,

  According to the property of inverse element,

  $$g \cdot g^{-1} = g^{-1} \cdot g = e$$

  The same equations show that g plays the role of an inverse for g^{-1}.

  Since the inverse element is unique, by **Property 2**, we can conclude that:

  $$(g^{-1})^{-1} = g$$

  This shows that the element is itself an inverse element of its inverse.

In addition, there are two more properties of groups:

- **Property 4: In any group, the inverse of the product of two elements equals to the product of the inverses of these two elements. (i.e. $(\boldsymbol{a \cdot b})^{-1} = \boldsymbol{b^{-1} \cdot a^{-1}}$)**
- **Property 5: In any group, two elements are equal if they are equal after being multiplied by another element. (i.e. If $\boldsymbol{ab = ac}$ or $\boldsymbol{ba = ca}$, then $\boldsymbol{b = c}$)**

You can have a go at proving these two properties, but guess what? By following the above proofs, you already get the hold of three basic theorems in group theory! Be patient though, there are more awaiting!

Example Group

Integers are a great example of a group formed with addition operation, which is expressed as $(\mathbb{Z}, +)$.

- Closure:
  - For any two of the integers a and b, $a + b$ is also an integer.
- Associativity:
  - For all integers a, b and c, they satisfy $a + (b + c) = (a + b) + c$.
- Identity element:
  - If a is any integer, $0 + a = a$ and $a + 0 = a$, thus 0 is the identity element of the group.
- Inverse element:
  - If a is any integer, $a + (-a) = 0$ and $(-a) + a = 0$, thus $(-a)$ is an inverse element of a.

Since all the rules are followed, integers with binary operation of $+$ is indeed a

group.

Lagrange Theorem

It would then be very useful to acknowledge the uses of group theory through Lagrange Theorem and its applications. Lagrange's theorem is probably one of the most famous theorems in group theory, and to understand it, we are required to learn a few more concepts for groups.

1. Subgroups

   Just like its name, subgroup simply means a group within a larger group. All the rules and axioms for groups are still applied on subgroups. As a result, all the subgroups contain the identity element of the group.

   It is equally important to note that, a group itself can be its own subgroup; similarly, the group's identity element can also be a subgroup with only one element, forming a trivial group. However, they are simply not quite interesting for us to work on.

   To find other subgroups, the most brutal way is to look through all the subsets within the group and mark out the subgroups. Nonetheless, the mathematicians are not patient enough the do the work and that is how Lagrange theorem is applied – it hugely narrows down the search area of subgroups.

2. Cosets

   Cosets are sets consisting of the products obtained from multiplying each element of the group G (including the elements within the subgroup), g, with each element within the subgroup H. The products can be either gH (named left cosets) or Hg (named right cosets).

So, you might ask, what on earth is Lagrange theorem? Well, Lagrange theorem points that the order (number of elements) of a subgroup must be a factor of the order of the group. I know this is not obvious, so let's go straight into proofs:

Let's first rewrite the theorem into symbols:

If $H \leq G$, $|H|$ divides $|G|$, where G is a finite group with $|G| = m$.

($H \leq G$ means H is a subgroup of G)

($|H|$ and $|G|$ means the order (the number of elements in the group) of H and G respectively)

Then we discuss the theorem in three different cases:

When $H = \{e\}$, $|H| = |\{e\}| = 1$, and 1 divides $|G|$, thus the theorem holds.

When $H = G$, $|H| = |G|$, and $|G|$ divides $|G|$, thus the theorem holds.

When $H \leq G$ and $H \neq \{e\}, G$, the case becomes slightly more complicated.

Here is what we are going to do:

Pick $g_1 \in G$ where $g_1 \notin H$, then $g_1 H$ does not overlap with H

This is because:

Assume $g_1 H$ overlaps with H, then $g_1 h_1 = h_2$ (for some $h_1, h_2 \in H$)

$$g_1 h_1 \cdot {h_1}^{-1} = h_2 \cdot {h_1}^{-1}$$

$$g_1 = h_2 \cdot {h_1}^{-1}$$

$$\because h_2 \cdot {h_1}^{-1} \in H$$

$$\therefore g_1 \in H$$

This contradicts the statement that $g_1 \notin H$

Therefore, when $g_1 \in G$ and $g_1 \notin H$, $g_1 H$ does not overlap with H.

After this, we carry on finding another coset $g_2 H$ and try to prove it does not overlap with other cosets (e.g. $g_1 H$).

Pick $g_2 \in G$ where $g_2 \notin H$, $g_2 \notin g_1 H$, then $g_2 H$ does not overlap with $g_1 H$

This is because:

Assume $g_2 H$ overlaps with $g_1 H$, then $g_2 h_2 = g_1 h_1$ (for some $h_1, h_2 \in H$)

$$g_2 h_2 \cdot {h_2}^{-1} = g_1 h_1 \cdot {h_2}^{-1}$$

$$g_2 = g_1 h_1 \cdot {h_2}^{-1}$$

$$\because h_1 \cdot {h_2}^{-1} \in H$$

$$\therefore g_1 h_1 \cdot {h_2}^{-1} \in g_1 H$$

$$\therefore g_2 \in g_1 H$$

This contradicts the statement that $g_2 \notin g_1 H$

Therefore, when $g_2 \in G$ and $g_2 \notin H$, $g_2 \notin g_1 H$, $g_2 H$ does not overlap with $g_1 H$.

We continue the same process until all the elements in H are used up and H

is split into non-overlapping left cosets.

Then, we will be surprised to find that all the left cosets we get have the same size!

Here is why:

$$H = \{h_1, h_2, \dots, h_k\}$$

$$gH = \{gh_1, gh_2, \dots, gh_k\}$$

The only situation such that $|gH| \neq |H|$ is when $gh_1 = gh_2$ for some $h_1 \neq h_2$ in H ($|gH| < |H|$)

Assume $gh_1 = gh_2$,

$$h_1 = h_2$$

This contradicts the fact that h_1 and h_2 are two distinct elements of H

Therefore, $|gH| = |H|$.

Since all the left cosets have the same size, let's call this size n; and say we have obtained p cosets. It is pretty clear that $|G| = p|H|$ (i.e. $m = pn$).

So, when $H < G$ and $H \neq \{e\}$, $|H|$ divides $|G|$, thus the theorem holds.

Since the theorem holds for all three cases, it is proved that the order of a subgroup must be a factor of its own group. In other words, congratulations, Lagrange theorem is now proved![3]

If you are into number theory, you might have heard of Pierre de Fermat, a crucial member of the constellation of mathematicians in 1600s. In his life, he enjoyed playing with his "little tricks" in numbers, and Fermat's Little Theorem is one of his inventions to kill boredom.

The theorem states that if p is a prime and a is any integer not divisible by p, then $a^{p-1} - 1$ is divisible by p,[4] and it can be proved using Lagrange's theorem.

Conclusion

Up to this point, I have explained in depth what group theory is through a basic

[3] Part of the ideas for proofs comes from: https://www.youtube.com/watch?v=TCcSZEL_3CQ&list=PLi01XoE8jYoi3SgnnGorR_XOW3IcK-TP6&index=7

[4] https://en.wikipedia.org/wiki/Fermat%27s_little_theorem

understanding of sets and groups, also including Lagrange theorem as it displays part of the applications of group theory in essence.

These concepts should open up the gate to a brand-new field of abstract algebra for you, and I hope that you have found them intriguing. They are not easy to understand, I know, but take your time, perhaps one day you will realise how amazing group theory and the abstract algebra are!