AN INTRODUCTION TO THE THEORY OF GROUPS

THOMAS L. KLIEM

This article will give a short outline on the theory of groups and should hopefully be accessible to the layperson.
Groups are one of the most fundamental aspects of higher level mathematics and aside from being the core element of abstract algebra they appear in nearly every aspect of pure mathematics.

We define a group as follows: $G = (G, *)$ is a group if

- G is a non-empty set of elements
- $*$ is an associative, closed, binary operation.
- There exists an identity element in G (often denoted e) such that for all g in G, we have $e * g = g = g * e$.
- For all elements g in G there exists an inverse (denoted g^{-1}) such that $g * g^{-1} = e = g^{-1} * g$.

I will expand on this definition by giving a basic example of group.

Consider the set of all integers, often denoted by $\mathbb{Z}$ from the German "Zahlen" for number. This set consists of all whole numbers ranging $\ldots, -4, -3, -2, -1, 0, 1, 2, 3, \ldots$ If we consider our operation $*$ to be the usual addition operator $+$ that we are familiar with then this forms a group $(\mathbb{Z}, +)$. We can inspect this group and prove our claim.
The operation $+$ is both associative and closed in this case. Associativity is the property that order of operations through brackets does not affect the end result. For any integers a, b, c we can see that $(a + b) + c = a + (b + c)$. The operation is also closed, meaning that if we add any two integers we will always arrive at another integer (another element of our set of elements $\mathbb{Z}$), i.e., we cannot add two whole numbers to arrive at a number which isn't also a whole number. We can also see that the $+$ operation is binary, i.e., that it involves exactly two elements.
To prove this is a group we then show that an identity exists and that inverses exist. The identity in this case is the number 0, as $a + 0 = a = 0 + a$, and that inverses exist and we have $a^{-1} = -a$, giving $a + (-a) = 0 = (-a) + a$.

Another infinite group you should be familiar with is the set of all real numbers, less zero, and the multiplication operation (which is denoted by $(\mathbb{R}\backslash\{0\}, \cdot)$) here we see that the product of any two non-zero reals is also a non-zero real, the identity is the number 1, and for any element x the inverse is $1/x$.

Thus we have our first basic examples of a group, and one that should be easy and familiar. There are some equally simple and easy to understand groups.

The trivial group consists of one element, the identity. This is the smallest possible group and to consider this you may think of the underlying set to consist only of the number 1, and the operation to be multiplication.

The next smallest group consists of two elements. There are multiple ways to consider this. You may think of it as the set $\{1, -1\}$ and the multiplication operation $*$. Again in this example the identity is the element 1 and every element is it's own inverse. Another way to consider this group is by thinking of $\mathbb{Z}_2$ under addition, or the integers modulo 2. This is a fancy way of saying that 2 is equivalent to 0.

This means we get the unfamiliar equation of $1 + 1 = 0$.

To make this clearer we can construct what is known as a group table, here are the group tables for the previous 3 groups.

$$T = \begin{array}{|c|c|}\hline * & e \\ \hline e & e \\ \hline \end{array}, \quad G_2 = \begin{array}{|c|cc|}\hline * & 1 & -1 \\ \hline 1 & 1 & -1 \\ -1 & -1 & 1 \\ \hline \end{array}, \quad \mathbb{Z}_2 = \begin{array}{|c|cc|}\hline + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \\ \hline \end{array}$$

If you look closely you can see the two groups with two elements are in similar. In fact these groups are considered isomorphic, which means they are identical up to labeling (this will be discussed later). In fact any group of size 2 must be isomorphic to this group (similarly there is only one trivial group of size 1).

One of the groups we have seen thus far gives rise to an infinite family of groups. In our $\mathbb{Z}_2$ group we can replace the 2 with any positive integer m to gain a group $\mathbb{Z}_m$ of that size, known as the cyclic group of order m. Cyclic groups can be considered as an operation on a polygon with m sides. For $\mathbb{Z}_4$ we consider rotation of a square with labelled corners, with the elements $0, 1, 2, 3$ being equivalent to rotating by $0°, 90°, 180°, 270°$ respectively. After each operation we still have a square, but the corners are now in different places; if we 'add' $1 + 3$ we get $90° + 270°$, which brings us back to our original position (noting that $3 = 1^{-1}$ in this group.)

Here I show the group tables for the cases where $m = 3$ and 4.

$$\mathbb{Z}_3 = \begin{array}{|c|ccc|}\hline + & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \\ \hline \end{array}, \quad \mathbb{Z}_4 = \begin{array}{|c|cccc|}\hline + & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \\ \hline \end{array}$$

Again the group of order 3 is unique up to isomorphism, however there are 2 non-isomorphic groups of size 4. The second is known as the Klein-4 group and is denoted as V_4.

$$V_4 = \begin{array}{|c|cccc|}\hline * & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & e & a \\ c & c & b & a & e \\ \hline \end{array}$$

If we wish to visualize this we can consider rotations and reflections of a non-symmetric figure. The identity (e) leaves it unaffected, one element (a) rotates 180° around the centre, another element (b) reflects down a vertical axis, and the 4th element (c) first rotates, then reflects. We can see that all a^2, b^2, and c^2 will bring us back to the original figure, and that the other relations $a * b = c$, $a * c = b$ etc hold.

One of the properties you may have noticed in all examples so far is that every group table is symmetric, or that every element commutes, that is to say that for all elements seen so far it hasn't mattered whether

we've gone $a * b$ or $b * a$ as $a * b = b * a$. This property is known as being 'abelian' and is true for all cyclic groups. There are however groups which do not possess this property. If we this time consider an equilateral triangle with labelled vertices and the operations of rotating each vertex one place (r) and holding one vertex while swapping the other two (s) we end up with this group table:

$$S_3 = \begin{array}{|c|cccccc|} \hline * & e & r & r^2 & s & rs & r^2s \\ \hline e & e & r & r^2 & s & rs & r^2s \\ r & r & r^2 & e & rs & r^2s & s \\ r^2 & r^2 & e & r & r^2s & s & rs \\ s & s & r^2s & rs & e & r^2 & r \\ rs & rs & s & r^2s & r & e & r^2 \\ r^2s & r^2s & rs & s & r^2 & r & e \\ \hline \end{array}$$

This group is known both as the Symmetric Group S_3 and the Dihedral Group D_6. The dihedral groups are the second major family we shall see and for each D_{2n} we have $2n$ elements acting as the rotations/reflections of an n sided polygon.

This should hopefully give you some insight as to what the definition of a group is and how it works.

Now we move onto some basic theorems and facts.

Theorem. Basic facts about groups:

(1) The identity element is unique
(2) Inverses are unique
(3) $(a^{-1})^{-1} = a$

Proof. (1) Suppose we have two identity elements e and e'. Then by the definition of identity we have that $e * e' = e$ and $e * e' = e'$ therefore $e = e'$

(2) Assume a has two inverses b and c then we have $a * b = e = c * a$ we get that

$$\begin{aligned} c &= c * e \\ &= c * (a * b) \\ &= (c * a) * b \\ &= e * b \\ &= b \end{aligned}$$

(3) By above a has a unique inverse a^{-1}. If we switch the roles of a and a^{-1} we see that a satisfies the definition of an inverse of a^{-1}.

□

Subgroups. An important concept in group theory is that of a subgroup. For anyone who's studied mathematics before a subgroup is what you'd expect. Given a group G a subgroup H consists of a subset of the original set G such that its elements form a group. This is equivalent to stating that the subset H is closed under the group operation $*$. We denote this $H \leq G$.

Example. Every group has two trivial subgroups. Firstly the group itself is considered a subgroup, secondly the identity element forms a subgroup isomorphic to the trivial group on one element.

Looking for more interesting examples we go back to our earlier group $\mathbb{Z}_4$, we see that if we consider only the elements $\{0, 2\}$ we create a subgroup isomorphic to $\mathbb{Z}_2$. (We check by inspecting closure and see that $0 + 0 = 0$, $0 + 2 = 2 + 0 = 2$ and $2 + 2 = 0$ are all members of our subgroup). This is the only

non-trivial subgroup of $\mathbb{Z}_4$, if we inspect V_4 we see that 3 non-trivial subgroups exist $\{e, a\}$, $\{e, b\}$, $\{e, c\}$. This acts as a proof that V_4 and $\mathbb{Z}_4$ are in fact different (non-isomorphic) groups of the same size.

Considering the group D_6 we can see four subgroups, one formed by taking only the rotation elements $\{0, r, r^2\}$ and three more by taking the symmetric element $\{0, s\}$, $\{0, rs\}$, $\{0, r^2s\}$. In fact for any dihedral group D_n we will find two subgroups one of the form $\{0, r, r^2, \ldots, r^{n-1}\}$ and the others being of the form $\{0, r^n s\}$ for values of n in the range $\{0, \ldots, n\}$

Homomorphisms and Isomorphisms. A homomorphism is a mapping from one group into another which preserves the group operation, that is for two groups $(G, *)$, $(H, \odot)$ and a mapping $f : G \to H$ we have for all a, b in G that $f(a * b) = f(a) \odot f(b)$. An isomorphism is a homomorphism that sends each element to a unique element.

Example. If we consider two groups from earlier $\mathbb{Z}_4$ and G_2 and the mapping:

$$f(0) = 1 \qquad f(1) = -1$$
$$f(2) = 1 \qquad f(3) = -1$$

Then this produces a homomorphism. We can check this easily e.g., $f(0 + 1) = f(1) = -1 = 1 * -1 = f(0) * f(1)$.
For an example of an isomorphism we use the group G_2 and $\mathbb{Z}_2$ and the mapping:

$$g(1) = 0 \qquad g(-1) = 1$$

This is clearly an isomorphism.

There are several facts about homomorphisms and isomorphisms but the only ones I will state here without proof are that any homomorphism $f : G \to H$ must send the identity element of G to the identity of H.
For any isomorphism the size of G and H must be equal.

Some other interesting groups:
Mentioned previously the symmetric group on n elements is denoted S_n and is the group of all permutations of n elements under composition. In fact every finite group can be presented as a subgroup of some symmetric group.
The general linear group of order n is the group of all invertible matrices of size n by n over some field F under matrix multiplication (given that you know what a field and matrix is this should be obviously a group).
The Rubik's Cube Group is the set of all possible moves on a Rubik's Cube with the composition operation (performing moves in a certain order). This group has size $43,252,003,274,389,856,000$.
However this pales in comparison to the Monster Group which has size

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

and was predicted to exist from theory several years prior to being computationally verified.