1 Introduction

In algebra we usually start with a set of objects and rules about how we are to combine these objects. We define a binary operation on a set S to be a function

$$\alpha : S \times S \to S \tag{1}$$

Note :Mathematicians represent maps between algebraic structures with the $\to$ but when they talk about maps between elements from one structure to another they use $\longmapsto$

The act of combining two elements is done by some binary operation $\star$ i.e a $\star$ b. This symbol will take different forms whether we will dealing with abelian groups i.e "+" or non-abelian groups ".". The simplest structure we can have before we arrive at groups is a **semigroup**, (S,$\star$). S is assumed to be non empty and the operation $\star$ is assumed to be associative i.e (a $\star$ b) $\star$ c = a $\star$(b $\star$ c). If in turn the semigroup has an identity element , e, such that a $\star$ e = a = e $\star$ a,then the semigroup is said to be a **monoid**. We then can add another level of structure and demand that the set have an inverse element such that $a{\star}a^{-1} = e$ for all $a \in$ S. When this is accomplished we have arrived at a **group**.

In summary we have the following definition of a group:
A group is a set, G, such that the following axioms are satisfied

1. The binary operation is associative
2. There is an identity element in the set
3. Every element has an inverse

1.1 Examples

1.Consider the set of natural numbers, $\mathbb{N}$. Supposing we exclude the number 0 from the set and have addition as our operation. Then we have a semigroup. If we include the number 0 then we have our additive identity and now $\mathbb{N}$ becomes a monoid. Note that the set of natural numbers can't be a group whether we choose addition or multiplication as our operation because if we choose addition we need the negative numbers for our inverses(which we do not have) but also if we choose multiplication as our operation 1 becomes the multiplicative identity but we do not have fractions in the set by definition.

2. A non mathematical example of a semigroup is the "renormalization group" in macroscopic lossy systems. Because we are loosing variables the operations need not have an inverse which means we need not have an identity element.

3.Consider the rotation of a regular polygon in rotated about an axis perpendicular to its plane of rest by angles $\frac{2\pi k}{n}$ where n is the number of sides and k is an integer less than n. The rotations form a group as we have the identity operation (namely do not rotate), inverse operation (rotate the other way) and clearly the rotations are associative

4.Supposing we have a set of n by n matrices with complex entries, $\mathbb{M}_n(\mathbb{C})$ or with real entries $\mathbb{M}_n(\mathbb{R})$. We need to form a group out of them, but run into an obstacle since not all matrices are invertible, in other words the inverses may not exist. We therefore restrict our selves to those that do and we denote them as $\mathbb{GL}_n(\mathbb{C})$ or $\mathbb{GL}_n(\mathbb{R})$

5. Consider the set of continuous invertible functions on the reals with one variable i.e f(x) which we denote as $Fun(\mathbb{R})$ with the operation of multiplication. These form a group.

1.2 Subgroups

It is often the case that when we have a set,S,that forms group we find out that there is a subset, N, that also obeys the axioms of the group. We call groups that arise from subsets that form groups, **subgroups**.

1.2.1 Examples and Motivations

1. The complex numbers $\mathbb{C}$ form a group but we can consider the real numbers $\mathbb{R}$ as a subset by making the imaginary part zero. But the real numbers form a group, so we can consider $\mathbb{R}$ as a subgroup of $\mathbb{C}$.

2. Consider the complex numbers on the unit circle $\mathbb{S}$ i.e $z = e^{i\theta}$ in the complex plane. These form a group but can be thought of a subgroup of $\mathbb{C}$

3. The set $(\mathbb{Z}, +)$ is a subset of the rational number with operation of addition $(\mathbb{Q}, +)$

Below is a proof that illustrates why considering a subgroup is important.

Theorem 1.1 *The group S_n (the group formed by the permutation of n objects) is abelian if and only if $n \leq 2$*

Proof We can directly prove that S_1 and S_2 are abelian. To do this let us introduced notation: $\pi = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots a_n \\ b_1 & b_2 & b_3 & \ldots b_n \end{pmatrix}$

The above means that we have a permutation π that takes the element a_1 to b_1 and a_2 to b_2 and so on.

For a specific example consider $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$

The above means we are dealing with the permutation of 5 objects with 1 permuted with 3, 3 permuted with 4 and 4 with 1. Meanwhile 2 is permuted with 5. A short hand notation then is $\pi = (134)(25)$. This permutation is just one element in S_5 that has 5! elements. The number of elements in a group is called its **order**.

Now let us consider S_2 which has elements $\pi_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ and $\pi_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ Clearly, π_1 is the identity element that keeps the objects where they are. Let us consider $\pi_1 \star \pi_2$, this gives π_2. Now consider $\pi_2 \star \pi_1$, π_2 exchanges the objects and

π_1 leaves them as they are i.e $\pi_2 \star \pi_1 = \pi_2$. It should be clear that S_1 is abelian since it only has one element. Now let us consider S_3 this has 6 elements (3!). Let's label them, $\pi_1 = (1)(2)(3), \pi_2 = (12)(3), \pi_3 = (13)(2), \pi_4 = (123), \pi_5 = (1)(23), \pi_6 = (132)$.

Now note that $\pi_2 \star \pi_4 = \pi_5$ but $\pi_4 \star \pi_2 = \pi_3$. In other words S_3 is nonabelian. Here now is the important point, S_3 is a subgroup for S_n with $n > 2$. It is impossible for a group to be abelian but one of its subgroups to be non-abelian so S_n with $n > 2$ is non-abelian. QED

This in general can be a strategy for deciding whether a group is abelian or not. Just pick a subgroup and investigate instead. Why? Subgroups are smaller.

1.3 Maps between Groups

In order to motivate the topic let us learn about the cayley table or the group multiplication table. This is a table that encodes how the group operation works among the group elements. Let us consider the rotations of square about the z axis by multiples of 90 degrees these form a group which we hence forth call R_4 and the integers modulo 4 which we call $\mathbb{Z}_4$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

*	R(0)	R(90)	R(180)	R(270)
R(0)	R(0)	R(90)	R(180)	R(270)
R(90)	R(90)	R(180)	R(270)	R(0)
R(180)	R(270)	R(0)	R(90)	R(180)
R(270)	R(0)	R(90)	R(180)	R(270)

Looking at the above table we see there is some sense in which these two groups are the same. In fact if we make the function $0 \to R(0)$, $1 \to R(90)$, $2 \to R(180)$, $3 \to R(270)$ we see that although these are two different groups their multiplication is identical. What we have found is called an isomorphism.

More formally a group **isomorphism** is a bijective function $\alpha : G \to H$ such that

$$\alpha(xy) = \alpha(x)\alpha(y) \tag{2}$$

where x,y $\in G$. Note that multiplication on the left side is in G while multiplication on the right is in H. This is important to note because the operations in these two groups might not be the same as in our example above. The idea behind this is that these groups are the same apart from labeling of the elements. We denote this relationship as $G \simeq H$

Let us suppose now that eq.2 still holds but that the map is no longer bijective. For this, consider two groups $\mathbb{Z}$ the group of integers and $\mathbb{Z}_3$ the integers modulo 3. Let α be the function $\alpha(x)$ = x mod 3 where $x \in \mathbb{Z}$ and $\alpha(x) \in \mathbb{Z}_3$. Clearly this is not a one to one map since all the multiples of 3 get mapped to 0 in $\mathbb{Z}_3$ nevertheless this map still obeys eq.2. Thus any function between two groups G and H that obeys eq.2 but is surjective (onto) is called a **homomorphism**.

1.4 Manipulating Group Elements

The following relate to manipulating group elements:

Theorem 1.2 *Let x, y, z be elements of G:*
1 . if $xy = z$ then $x = zy^{-1}$
2 . $(xy)^{-1} = y^{-1}x^{-1}$

Proof If xy = z then $(xy)y^{-1} = zy^{-1} \Rightarrow x = yz^{-1}$ by associativity. To prove the second statement we show that $y^{-1}x^{-1}$ is the inverse of (xy). $(xy)y^{-1}x^{-1} = 1$ and $y^{-1}x^{-1}(xy) = 1$

The next theorem relates the powers of groups

Theorem 1.3 *Let x be an element of a group G, and m,n be integers*
1. $x^m x^n = x^{m+n}$
2. $(x^m)^n = x^{mn}$

Proof We prove the first part by induction. Note that for m=n=1 we have that $xx = x^2$. We then assume the statement and then consider $x^m x^n x = x^m x^{n+1}$ by the induction step and therefore $x^m x^{n+1} = x^{m+n+1}$ by induction step again. Same can be done for negative powers.
We prove the second part by induction. The statement is true when n=0. We make the induction step and do the calculation $(x^m)^{n+1} = x^{mn}x^m$ by induction step and that is equal to $x^{m(n+1)}$ by the first part of the theorem.

1.5 A Group as a Permutation

Looking at the Cayley tables in the previous section we note one obvious thing which can be turned into a theorem that is astounding. Note that the group multiplication in each row of the Cayley table simply permuted the elements around. The permutation in the Cayley tables shown is simple since the groups we chose were abelian but if they were not the permutations would have looked non-trivial. What is being stated here in a round about fashion is what is called the rearrangement theorem. But we could do better and make this a statement about groups. The theorem is as follows:

Theorem 1.4 *Every group is isomorphic to a permutation group or is in general a subgroup group of the symmetric group S_n where n is the order of the group.*

Proof We begin by defining a function $\pi_a : G \to G$ as follows

$$\pi_a(x) = ax. \tag{3}$$

The operation on the left side is assumed to be group multiplication. The goal is to show that this function is an isomorphism. Clearly unless a is the identity it will take a to some other element so that we can imagine a row of group element and the action of this function will be to switch the elements around.

1. The function is injective: Suppose $\pi_a(x_1) = \pi_a(x_2)$ then we have that $ax_1 = ax_2$. Both sides can be multiplied by a_1^{-1} to give $x_1 = x_2$.
2. The function is surjective: $y = a(a^{-1}y) = \pi_a(a^{-1}y)$
So the function is an isomorphism and therefore we have that it is a permutation.

To show that it is a group, we must show that this permutation is closed under the group operation which will be composition, that it has an inverse.
1. The function is closed under compositions: $\pi_a(\pi_b(x)) = \pi_a(bx) = (ab)x = \pi_{ab}(x)$
2. Closed under inversions: Consider $\pi_{a^{-1}}(x) = a^{-1}x$ This is the inverse of π_a since $\pi_{a^{-1}}(\pi_a(x)) = \pi_{a^{-1}}(ax) = (a^{-1}a)x = x$

Now since the map π_a does not give all the permutations of all the elements in G, we must have produced a subgroup of S_n. QED

2 Structure of Groups Analyzed via Subgroups

In the previous section we introduced the idea of a group and gave examples all of them being concrete examples. In fact all of the examples are encountered in other areas of mathematics, physics and chemistry and can be mostly be studied without reference to their group nature. What was noticed early in the history of group theory was that it is possible to abstract out the essential properties of a group and study them separately without reference to a realization of the groups. So for example instead of studying $\mathbb{Z}_2, \mathbb{Z}_3$ or in general $\mathbb{Z}_n$ we can abstract out the properties in all these groups and study them without reference to how they are materialized in $\mathbb{Z}_n$. These groups are examples of what is called a **cyclic group**.

Our goal in this section is to analyze the structure of groups mainly by investigating the kinds of subgroups that might arise. In section 1.1.2 we saw how examining a subgroup gave us valuable information about the group itself. Before we move towards this goal we first introduce cyclic groups as an example of talking about groups in the abstract.

2.1 Cyclic groups

These groups are formed by taking all the powers of an element x in a group G. Since the group is closed under the operation all the powers will be in G and therefore we will obtain a subgroup of G. The group is denoted as $< x >$. Now since a subgroup containing x must contain all the powers of x it follows that $< x >$is the smallest subgroup containing x. If the group G is generated by $< x >$ the G is said to be **cyclic**. Examples include $\mathbf{Z} =< 1 >$ or $\mathbf{Z}_n =< [1]_n >$

We can prove that $\mathbb{Z}_n$ is isomorphic to a cyclic group of order n. We already know this to be true but for fun we can assume that we just have a set consisting of elements in $\mathbb{Z}_n$ and show it is isomorphic to a cyclic group G.

Theorem 2.1 *$\mathbb{Z}_n \simeq G$ with G being cyclic and of order n.*

Proof Create the function $\alpha : \mathbf{Z}_n \rightarrow G$ as $\alpha([i]) = x^i$. This function is well defined and moreover bijective. If we allow $\mathbf{Z}_n$ to be written additively and G multiplicatively. We are done.

Theorem 2.2 *Every subgroup of a cyclic group is a cyclic group.*

Proof Let G be cyclic group and H be a subgroup. Since G is a cyclic group it is generated by one element say, a. Which means that the elements of H are some power of a.Let a be the smallest power such that a^m generates H. The task is now to show that every element of H is a power of a^m. Let t be an integer greater than m and apply the division algorithm so that $a^t = a^{mq+r}$ where r is less than m. We can rewrite this as $a^r = a^{-mq}a^t$ but we decided that m was the lowest power so r must be 0 and therefore $a^t = a^{mq}$ as desired. QED

We can generalize the notion of a cyclic group by noting that if $\{H_i | i \in \Lambda\}$ is a set of subgroups of a group G, then $\bigcap_{i\in\Lambda} H_i$ is also a subgroup. We then get a set X in G and collect all the subgroups that contain X. This will form another subgroup and it is denoted as $< X >$.

We now show how the subgroup $< X >$ generalizes the idea of a cyclic group by proving the following theorem.

Theorem 2.3 *Let X be a non-empty subset of the group G. Then$< X >$ consists of all elements of G of the form $x_1^{\epsilon_1} x_2^{\epsilon_2} \ldots x_k^{\epsilon_k}$ where $x_i \in X, \epsilon_i = \pm 1$ and $k \geq 0$.*

Proof Let S denote the set of all the elements of the specified type. It can be easily be checked that S becomes a group. Now X ⊂ S and in fact $< X >\subset S$ since $< X >$ is the smallest group that containing X. On other hand the elements $x_1^{\epsilon_1} x_2^{\epsilon_2} \ldots x_k^{\epsilon_k}$ must belong to X since $x_i \in X$ so $S \subset< X >$. The only way to sets can contain each other is if they are in fact the same. QED.

2.1.1 Order of a group element

Let x be an element of a group. If the subgroup $< x >$ contains a finite number of elements n, the x is said to have a *finte order m* while is $< x >$ has an infinite number of elements then x is said to have *infinite order*.

The following theorem contains the basic facts pertaining to the order of an element.

Theorem 2.4 *Let x be an element of a group G.*
i) if x has infinite order then all the elements of G are distinct
ii) if x has finite order m, then m is the least positive integer m such that $x^m = 1$ and $< x >$ consists of distinct elements $1, x, x^2, \dots x^{m-1}$
iii) if x has finite order and $x^l = 1$ if and if only l is divisible by m.

Proof By the well ordering principle there is a least integer m such that $x^m = 1$. Suppose there is another integer $l > m$ such that $x^l = 1$ then by the division algorithm we have that $x^l = x^{mq+r}$ for some q and r less than l and r less than m. Thus we have that $x^l = x^r$. So if $x^l = 1$ we must have that r= 0 and therefore iii) is established. But we have established more since if $x^l = x^r$ it must mean that $< x >= \{1, x, x^2 \dots x^{m-1}\}$ are all distinct and so ii) is established. It should be clear that if the order of x is infinite then we can extract from the above arguments that all powers of x must be distinct. QED

2.2 Cosets and Lagrange's Theorem

2.2.1 Partitions and Equivalence relations

Before we consider what cosets are let us investigate the relation between a partition and an equivalence relation because cosets are partitions of a group induced by a certain equivalence relation.

So when we say that we have partitioned a group we mean that we have divided it up into distinct subsets all of which are disjoint. More formally speaking a **partition** of a set is a family of $\{A_i : i \in I\}$ of nonempty subsets of A which are mutually disjoint and whose union is all of A. Thus should you find an element x that lies in the subset A_i and A_j you can immediately conclude that these two subsets are in fact the same subset and there should be no element that does not belong to a class or subset.

Putting aside the notion of a partition for now, we consider another notion namely an equivalence relation. First of all, what is a relation? A **relation** is a true or false statement relating two elements a and b from a set.We denote this in general as $a \sim b$ A relation is said to be an **equivalence relation** if the following three things hold:

1. $x \sim x$ reflexive property
2 . if $x \sim y$ then $y \sim x$ symmetric property
3. if $x \sim y$ and $y \sim z$ then $x \sim z$

A physics example is the notion of thermal equilibrium because:

1. Any system A is in thermal equilibrium with itself
2. If system A is in thermal equilibrium with B then B is in thermal equilibrium with A.
3. If system A is in thermal equilibrium with B and B is in thermal equilibrium C then A is in thermal equilibrium with C.

Thus the notion of thermal equilibrium is an equivalence relation. Another example of an equivalence relation is the notion of equality. It should now be clear that a partition is in fact an equivalence relation. Why?

1. Every x in a set A is an element of one and only one partition A_i so $x \sim x$
2. If x and y are in the same partition then we say that $x \sim y$ and clearly $y \sim x$
3. If x is the same partition as y namely A_i and y is some partition A_j as z. Then it must mean that x and z are in the same partition so $A_i = A_j$ and $x \sim z$

In the following theorem we formalize the intuition.

Theorem 2.5 *If $\sim$ is an equivalence relation on A, the family of equivalence classes, $\{[x] : x \in A\}$ of is a partition of A. Where x acts as a representative element for the class*

Proof We define the equivalence class of an element x as $[x] = \{a \in A|\text{where } a \sim x\}$. By the reflexive property $x \in [x]$ and therefore $A = \bigcup_{x \in A}[x]$. So A is a union of equivalence classes.

We now show that these classes are disjoint. Suppose that $[x_1]$ and $[x_2]$ both contain b and $a \in [x_1]$. Then we have that $a \sim x_1, b \sim x_1$and $b \sim x_2$ by the symmetric property. So $[x_1] \subset [x_2]$ since $a \in [x_2]$. We can also run the argument the other way round to show that $[x_2] \subset [x_1]$ and therefore these are in fact the same class.So no two equivalence classes can share the same element "a" and we have therefore partitioned the set. QED

2.2.2 Cosets

Consider a group G with subgroup H and define the relation $x = yh$ with $x, y \in G$ and $h \in H$. So $x \sim_H y$. This is an equivalence relation since

.1 $x = xe$ with $x \in G$ and $e \in H$, e is the identity in H.
2. $y = xh^{-1}$ so $y \sim_H x$
3. $x = yh$ and $y = zh_1 \Rightarrow x = zhh_1$ so $x \sim z$

What we have define is called the left coset and is the set of elements

$$\{xh \mid \in H\} \tag{4}$$

The coset is denoted as

$$xH \tag{5}$$

So the left cosets partition the group and also note that the only coset that is a group is eH, where e is the identity element since no other coset apart from this contains the identity element. Also we have a bijection from H to xH defined by $h \longmapsto xh(h \in H)$ since if $xh_1 = xh_2$ then this implies that $h_1 = h_2$. From this it follows that the order of any left coset is equal to the order of the subgroup H. The same exercise can be done for right cosets. Note that if the group is abelian then the right cosets and the left cosets will be the same otherwise they in general will not be.

2.2.3 Lagrange's Theorem

Theorem 2.6 *(Lagrange's Theorem)Let G be a group and H be one of its subgroup. Then the order of H, $|H|$ divides the order G, $|G|$ moreover $\frac{|G|}{|H|}$ = the number of left cosets = number of right cosets*

Proof To prove this simply count the number of left cosets you have in your group.Say there are n of them. Since they are all distinct it is a simple matter to note that $|G| = n|H|$ or $\frac{|G|}{|H|} = n$. It should be clear that we could have formed right cosets instead and had we gone through the same argument the answers would agree. QED

As a consequence we have arrived at an important fact. Namely, the order of a subgroup divides the order of a group. Why is this important? Because the order of the subgroups in a group is equal to the divisors for the order of the group. For example a group of order 6 can only have **proper subgroups** of order 3 and 2. Proper subgroups are those that are not the identity element or the group itself.

(REMARK: If the operation of the group is "+" is often the custom to denote the left cosets for example as x + H rather than xH.)

2.2.4 Examples of cosets

1.Consider ($\mathbb{Z}$, +) and set the subgroup to be ($3\mathbb{Z}$,+) The cosets are $3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z}$. In general for the group under discussion and subgroup ($m\mathbb{Z}$,+), the cosets are $m\mathbb{Z}, 1+m\mathbb{Z}, 2+m\mathbb{Z}\ldots(m-1)+m\mathbb{Z}$

2.Let $G = S_3$ and $H =< (12)(3) >$. First we find out what the subgroup looks like. Let $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ then $\pi^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ so π^2 is the identity permutation (id) which means the group is of order 2. The group is not of infinite order so we Lagrange's theorem and get that it must have three left cosets. They are $H = \{id, (12)(3)\}, (123)H = \{(123), (13)(2)\}, (132)H = \{(132), (1)(23)\}$ We proved earlier that S_3 is non abelian so we must have right cosets be different: $H = \{id, (12)(3)\}, H(123) = \{(123), (1)(23)\}, H(132) = \{(132), (13)(2)\}$

3. Consider the set of vectors x in $\mathbb{R}^n$ such that $Ax = 0$ where A is some n by b matrix. This is indeed a group as can be easily checked. They form a vector space which we will call V. Now consider the solution x which is a solution to $Ax = b$ concretely let us call it x_0. This gives a coset $x_0 + V$ in $\mathbb{R}^n$ which describes the set of solutions to $Ax = b$

4. Lastly we can consider the symmetries of an equilateral triangle. We list the group elements first:
a) e : do nothing
b) a : rotate by 120
c) b :rotate by 240
d) X: reflect through first perpendicular bisector whatever you choose it to be.
e) Y: reflect through second perpendicular bisector whatever you choose it to be
f) Z : reflect through third perpendicular bisector whatever you choose it to be

We reproduce the multiplication table of the group

*	e	a	b	X	Y	Z
e	e	a	b	X	Y	Z
a	a	b	e	Y	Z	X
b	b	e	a	Z	X	Y
X	X	Z	Y	e	b	a
Y	Y	X	Z	a	e	b
Z	Z	Y	X	b	a	e

Let us pick the subgroup to be that which contains the rotations so $H = \{e, a, b\}$. This is of order 3 so we expect 2 cosets. Let us look at the left cosets: $H = \{e, a, b\}, XH = \{X, Z, Y\}, YH = \{Y, X, Z\}, ZH = \{Z, Y, X\}$. Note we only get two distinct cosets. According to Lagrange's theorem there should be groups of order 2. Looking at the table it should be clear what they are.
The group be we have described is an example of groups called the Dihedral groups. These groups describe the symmetries of regular polygon. They are of order 2n for an n-sided polygon. A good exercise to look at the square and identify the subgroups and cosets of each subgroup.

2.2.5 Some consequences of Lagrange's Theorem

Theorem 2.7 *The order of any element of a finite group divides the order of the group.*

Proof We already know that the order of the subgroup must divide the order of the group. When we look at an element of the group, we know that the order is the least positive integer m such that $x^m = 1$. But such an element will produce a cyclic subgroup of order m, so the order of an element must divide the order of the group. QED

Corollary 2.8 *A little thought should convince the reader that if the order of the group is n then $x^n = 1$ for every $x \in G$*

Theorem 2.9 *Let G have order pq where p and q are prime then either G is cyclic or every element $x \neq e \in G$ has order p or q.*

Proof The possible proper subgroups are those of order p and q but if this is the case then G can't be cyclic because the only possible order of an element in the subgroup is either p or q (remember the order of the element must divide the group) and therefore every element not equal to the identity must have order p or q. The other option is that G has no proper subgroup and is generated by one element of order pq. QED.

2.3 Normal Subgroups and Quotient Subgroups

2.3.1 More Careful look at homomorphisms

We introduced what a homomorphism was in the introductory section, we now take a more careful look at them. The best we can hope for is an isomorphism between groups but if that is not the case, we can still have maps the preserve the "structure" of a group as they transform it from one to another. What it means is this: Say we have two groups G and H and a homomorphism ϕ from G to H. Then $\phi(a) = a'$ and $\phi(b) = b'$ then $\phi(ab) = a'b'$. When the map is onto we say the H is the homomorphic image of G. If the group is abelian one might see the homomorphism expressed as $\phi(a+b) = \phi(a) + \phi(b)$. We now prove some theorems on homomorphism that give more insight into its nature.

Theorem 2.10 *Let G and H be groups and f: $G \to H$ a homomorphism. Then*
i) f(e) = e
ii) $f(a^{-1}) = [f(a)]^{-1}$

Proof In any group if we have yy= e then y=e. So f(e)=f(ee)= f(e)f(e) means f(e)=e. This proves the first part. For the second note that $f(e) = f(aa^{-1}) = f(a)f(a^-1) \Rightarrow f(a^{-1}) = (f(a))^{-1}$ QED

The **Kernel** of a map f are all the elements that are map from one group G to the identity element H by the homomorphism f.

We list some elementary properties of homomorphisms.

1. If $f : G \to H$ and $g : H \to K$ are homomorphism then their composition is a homomorphism from from G to K.
2.The homomorphism $f : G \to H$ is injective if the Kernel is just the identity element.
3.If $f : G \to H$ is a homomorphism and K is any subgroup of G, then f(K) is a subgroup of H.

2.3.2 Normal Subgroups

Normal subgroups are important because they help us construct other groups namely Quotient groups. But first we define them, study them and give examples.

Theorem 2.11 *Let H be a subgroup of a group G. Then the following statements about H are equivalent:*
i) xH = Hx for all x in G.
ii)$xhx^{-1} \in H$ whenever $h \in H$ and $g \in G$

The element xhx^{-1} is called the conjugate of h by x.

Proof We assume i) holds and then prove i). From one we have that $xh = h_1x$ for $x \in G$ and $h, h_1 \in H$ We multiply both sides by x^{-1} to get $xhx^{-1} = h_1 \in H$. Next we assume ii) holds. From the first part of the proof we have that $xhx^{-1} = h_1 \Rightarrow xh = xh_1$ so $xH \subset Hx$.. Also we have that $x^{-1}h(x^{-1})^{-1} = h_2 \Rightarrow h(x^{-1})^{-1} = xh_2 \Rightarrow Hx \subset xH$ and thus xH = Hx

A subgroup that has the properties above is called a normal subgroup. We have already seen a normal subgroup.
1.In investing the cosets of the Dihedral group of a triangle we chose a subgroup that was in fact normal.
2. Another example is $\mathbb{SL}_n(\mathbb{R})$ in the group $\mathbb{GL}_n(\mathbb{R})$. To see why merely look at the determinant of ABA^{-1} with $A \in \mathbb{SL}_n(\mathbb{R})$ and $B \in \mathbb{GL}_n(\mathbb{R})$. You should find the determinant of the resulting matrix to be 1.
3. The abelian group of translation is a normal subgroup of the Poincare group.
4. The center of a group G denoted as Z(G) -(all the elements that commute with every other element in the group) is a normal subgroup
5. Denote the element $xyx^{-1}y^{-1}$ as $[x, y]$. This is called the commutator since it is 1 only when the group is abelian.The **derived subgroup** $G^{'}$ is the group generated by all the commutators.Calculating $z[x, y]z^{-1}$ shows that this is equal to $[zxz^{-1}, zyz^{-1}]$ so the derived subgroup is a normal subgroup.

(REMARK:Since we have mentioned equivalence classes in some depth, it is easily shown that the conjugate relation xgx^-1 is in fact an equivalence relation. It should make intuitive sense then (given the definition of a normal group) that it is a union of conjugacy classes.)

2.3.3 Quotient Groups

In the previous section we saw cosets for the first time and used them to prove Lagrange's theorem. We also noted that they formed equivalence classes, it is this property that then inspires the notion of quotient groups. Since we have equivalence classes we ask ourselves whether it is possible to think of the cosets as a an element in some kind of group i.e is there a sense in which all the elements in a coset act in unison so that we can think of them as essentially one element? If this works out, we must have elements from one coset multiplying elements from another coset and giving us another element in a different coset. So what we want is something like this:

$$(xH)(yH) = zH \text{ where } z = xy \tag{6}$$

Starring at the equation above we see that any old subgroup of the group will not do. It must be the case that xH = Hx for the above formula to work. But we have already come across such subgroups they are our normal subgroups from the section before. So we have come across an important fact in order to produce a group out of the cosets we need to have our subgroup H to be normal.

Once we define an operation it is important that we check that it is well defined in this case that the operation does not depend on what member of the cosets we chose. This would be the next step in any rigorous treatment of the subject we omit here.

Once all that has been done we have arrived at the **Quotient group** denoted as G/H

A few examples are :
1. Pick the identity element(1) and consider it a normal subgroup, the $G/1$ is a quotient group. This is not a new group but in fact the G that we started off with.
2. We saw earlier the group $(n\mathbb{Z}, +)$, it should be easy to prove that it is a normal subgroup. Now create the Quotient subgroup $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$. To see this pick an element in the normal subgroup,$n\mathbb{Z}$, and create a coset. namely, $x + nq|q \in \mathbb{Z}$. Notice that adding two different cosets is tantamount to adding modulo n in other words we are in $\mathbb{Z}_n$
3. $G/G^{'}$ is an abelian quotient group . Remember G' is the derived subgroup. 4. The circle group (G): this consists of rotations by $2r'\pi$ where $r' \in \mathbb{R}$. We show that this is a quotient group by defining the map $\beta : \mathbb{R}/Z \to G : r+\mathbb{Z} \longmapsto r'$ and showing that this map is in fact an isomorphism. First we show that the map in injective and this is so because suppose $r'_1 = r'_2 \Rightarrow 2r'_1\pi = 2r'_2 + 2n\pi$ for $n \in \mathbb{Z}$ (Since r' + n = r') so $r'_1+\mathbb{Z} = r'_2+\mathbb{Z}$. Second the map is clearly surjective. So we have a bijective map on our hand. It should be easy to prove that this bijective map is actually a homomorphism and therefore we have an isomorphism on our hand.
5. Pick D_3 the dihedral group of the equilateral triangle and then pick the normal subgroup to be that formed from the rotations R_3. We saw earlier that we got only two distinct cosets. The quotient group $D_3/R_3 \simeq \mathbb{Z}_2$

2.4 Isomorphism Theorems

Now that we have seen quotient groups and are familiar with homomorphisms we are in a position to prove the three isomorphism theorems. These three theorems appear in different guises in the theory of rings, lie algebras and vector spaces.

Theorem 2.12 *(First Isomorphism theorem) If $\alpha :\to G \to H$ is a homomorphism between groups then $G/Ker(\alpha) \simeq Im(\alpha)$ via the mapping $xKer(\alpha) \longmapsto \alpha(x)$*

Proof We define the map $\beta : G/K \to Im(\alpha)$ where $K = Ker(\alpha)$ by the rule $\beta(xKer(\alpha)) = \alpha(x)$. This map is well defined (must be checked). The map β is a homomorphism since $\beta(xyKer(\alpha)) = \alpha(xy) = \alpha(x)\alpha(y) = \beta(xK)\beta(yK)$. So $Im(\beta) = Im(\alpha)$ and moreover $\beta(xK) = 1_H$ if and only if $x \in K$. Thus β is an isomorphism

Theorem 2.13 *(Second Isomorphism theorem) Let G be a group with a subgroup H and a normal subgroup N. Then* $HN \leq G, H \bigcap N \lhd H$ *and* $HN/N \simeq H/H \bigcap N$

Proof Define the map $\Theta : H \to G/N$. This map takes the element h to one of the cosets i.e $h \longmapsto hN$ thus $HN \leq G$ and therefore $Im(\Theta) \simeq HN/N$. Now an element $h \in Ker(\Theta)$ if and only if $h \in N \Rightarrow h \in H \bigcap N$ and so by the first isomorphism theorem we have that $H/H \bigcap N \simeq HN/N$

Theorem 2.14 *(Third Isomorphism theorem) Let M and N be normal subgroups of a group G such that* $N \subseteq M$*. Then* $M/N \lhd G/N$ *and* $(G/N)/(M/N) \simeq G/M$

Lemma 2.15 *If* $\alpha : G \to H$ *is a homomorphism the image* $Im(\alpha)$ *is a subgroup of H annd the kernel* $Ker(\alpha)$ *is the normal subgroup of G.*

Proof From the properties of homomorphism listed earlier we know that the image of a homomorphism is a subgroup. We also have that $Ker(\alpha)$ is a subgroup of G since for $x, y \in Ker(\alpha)$ we have $\alpha(x)\alpha(y) = \alpha(xy) = 1_H 1_H = 1_H$ and $\alpha(x^{-1}) = (\alpha(x))^{-1} = 1_H^{-1} = 1_H$. It remains to prove that the kernel is a normal subgroup, which is done by noting $\alpha(xgx^{-1}) = \alpha(x)\alpha(g)\alpha(x)^-1 = \alpha(x)\alpha(x)^{-1} = 1_H$ for $x \in G$ and $g \in Ker(\alpha)$

Proof We begin with a short proof. Define the map $\Theta : G/N \to G/M$ by $\Theta(xN) = xM$. The kernel of this map is M/N. The theorem then follows by the first isomorphism theorem and the lemma.

A second and more intuitive proof is to define a series of maps thusly:

Proof Version 2: Define a map $G \to G/M$. This takes $x \longmapsto xM$. Then define another map $\beta : G/M \to (G/M)/(M/N)$, this maps $xM \longmapsto (xM)(yN)$ with $y \in M$. Then we ask what the kernel of the map $\beta \circ \alpha$ is. Some thought shows that the kernel are the elements in N. So the result follows by the first isomorphism theorem.

3 Group Actions

Having studied the basics of groups in the abstract, we then turn around and study them by finding a way of representing them as some concrete objects (What is meant by "concrete" will be made more precise). The way to do this has already been introduced when we proved that a group can be considered as a subgroup of S_n. It might seem strange we developed a whole abstract theory of groups and now are turning around and describing them as concrete objects. One reason this might be a good thing to do is that it makes studying a specific group easier. We might be handed some group and are asked to study it more carefully. A lot of the analysis can be accomplished by imagining it as a representation of some concrete thing.

Since we have already proved Cayley's theorem (Theorem 1.1.4) it should not be surprising that we want to represent the group as a group permutations of a set. Once we do this, we say the group **acts** on the set.

3.1 Permutation Representation

Let G be a group and X be some non empty set, we define the function

$$\alpha : G \times X \to X$$

written as $\alpha((g, x)) = g \star x$ such that

1. $g_1(g_2) \star x = (g_1 g_2) \star x$
2. $1_G \star x = x$

What we have defined above is the *left action* on the set X. A corresponding definition can be given for the right action. We aim to assign to every element in G a permutation on the set X in such a way that the identity element is assigned to the identity permutation and the group product gk is assigned the composition of permutation elements assigned to g and k. More abstractly what we are doing is defining a homomorphism $\beta : G \to Sym(X)$ where Sym(X) is the set of all permutations on the set X. This is called the *permutation representation* of G on X.

Notice we defined the group action on x with the star and that is because there are many ways that a group can be considered as acting on a set.

1. We can have group action by multiplication. A realization of this is if the group G acts on its underlying set G i.e $g \star x = gx$. It can be easily shown that this is in fact a left action. When we have the group acting on its underlying set we have what is called the *left regular representation.*

(Note: One of the properties mentioned earlier was that a homomorphism was injective if its kernel consisted of just the identity element. If the homomorphism is surjective then we have a bijection. To apply this to the current situation note that if the homomorphism $\gamma : G \to Sym(G)$ has the kernel consisting only of the identity element then we have proved Cayley's theorem)

2. Action by conjugation. We can define $g \star x = gxg^{-1}$. Again interesting results ensue if we ask what the kernel is . Clearly then kernel consists of the those elements in G such that $xgx^{-1} = x$ i.e the elements in the center of the group, Z(G). The *center* of the group consists of the elements in the group that commute with all other elements in the group. Thus it follows that Z(G) is the kernel of the conjugation representation.
3. Action on cosets: The left action on the cosets is defined by the rule $g \star (xH) = (gx)H$.Consider the permutation representation $\alpha : G \to Sym(\mathcal{L})$ where $\mathcal{L}$ is the set of left cosets. Again we ask how the kernel looks like. If g is in

the kernel it must be that (gx)H = xH i.e $x^{-1}gx \in H$ So $Ker(\alpha) = \bigcap_{x \in G} xHx^{-1}$

4. Lastly we give an explicit example of the permutation representation with the group D_3. Label the vertices of a triangle with 1,2,3 anticlockwise and rotate anticlockwise
i) e→ (1)(2)(3)
ii) 120 rotation → (312)
ii) 240 rotation → (321)
iii) The three reflection correspond to (1)(23),(2)(13),(3)(12)

3.2 Orbits and Stabilizers

Given a group G and a non empty set X let's suppose we have a left action on X. Then a binary relation $a \sim_G b$ defined on X is defined by the rule:

$$a \sim_G b \text{ if and only if } g \star a = b$$

for some $g \in G$. It is easily verifiable that the binary relation defined above is an equivalence relation.

The equivalence class containing a is:

$$G \star a = \{g \star a | g \in G\}$$

and is called the **G − orbit** of a. So is a union of disjoint orbits. If there is only one orbit in the set X, then the action of the permutation on X is said to be **transitive**. Examples of this include:
1. the permutation representation of D_n on the vertices of an polygon. The whole set can be reproduced by the permutation acting on only one element (vertex).
2.Action of S_n of $\{1, 2, \ldots n\}$ since there is a permutation that will take 1 to every element in the set.
3. The left regular representation is transitive
4. The left action of the set of left cosets.

Another concept is called **stabilizer**. The stabilizer in G of an element $a \in X$ is defined to be

$$St_G(x) = \{g \in G | g \star x = x\}$$

$St_G(a)$ is a group.
Examples of stabilizers:

1. For the conjugation action of G on G the stabilizer of x in G is all of g such that $gxg^{-1} = x$. This group is called the **centralizer** of x in G.

$$C_G(x) = \{g \in G | gx = xg\}$$

2.In the action of G by conjugation on it set of subgroups, the G-orbits of H $\leq G$ is the set of all conjugates of H in G i.e $gHg^{-1}|g \in G.$ This is stabilizer of H in G is a subgroup called the **normalizer** of H in G.

$$N_G(H) = \{g \in G|gHg^{-1} = H\}$$

-