Group

In abstract algebra a group $(G, *)$ is a tuple of a set with binary multiplication $* : G \times G \to G$ such that the following rules hold:

1. **Associativity**: For any element $a, b, c \in G$, $(a * b) * c = a * (b * c)$.

2. **Identity**: There exists an element $e \in G$ with the property that $e * g = g * e = g$ for every element $g \in G$.

3. **Inverses**: For any element $g \in G$ there exists an element $g^{-1} \in G$ such that $g^{-1} * g = g * g^{-1} = e$.

This is a simple structure one can put on a set that proves extremely useful in many different areas of mathematics and physics. We will prove some basic facts about a group:

Uniqueness of identity

Suppose there are two identity elements $e, e' \in G$ by definition

$$e' = e * e' = e$$

So we get $e' = e$, and we've shown the uniqueness of the identity.

Uniqueness of the inverse

Let $g \in G$ be an arbitrary group element. Assume there are two inverses for g, call them h, h'.

$$h' = (h * g) * h' = h * (g * h') = h$$

So we get that $h = h'$, implying the uniqueness of the inverse of an element.

$\square$

Definition: The *order* of a group $(G, *)$ denoted $|G|$ is the cardinality of the set G.

Definition: The order of an element $g \in G$, is the smallest natural number $m \in \mathbb{N}$ such that $g^m = e$. We denote the order of an element $\operatorname{ord}(g)$.

Definition: A subset $H \subseteq G$ is called a *subgroup* of G if

1. Contains the identity: $e_G \in H$
2. Inverses of elements in H are in H, i.e. if $h \in H$ then $h^{-1} \in H$.
3. Closure: if $g, h \in H$ then $g * h \in H$.

We write $H \leq G$ when H is a subgroup of G.

Note: A Group is called ***Abelian*** if the multiplication is commutative. i.e $\forall g, h \in G$, $g * h = h * g$.

1. Group homomorphisms

Whenever discussing a mathematical structure, we are of course also interested in studying the structure preserving maps between these structure (see Category Theory). In Group theory the structure that needs to be preserved is the multiplication. Let $(G, *_G)$ and $(H, *_H)$ be two groups. A mapping

$$\varphi : G \longrightarrow H$$

Is called a group homomorphism, if whenever $f, g \in G$ then $\varphi(f *_G g) = \varphi(f) *_H \varphi(g)$. From these the following corollaries hold about a homomorphism φ

1. Let e_G and e_H be the unique identity elements of G and H respectively, then $\varphi(e_G) = e_H$.

2. Let $g \in G$ be some arbitrary element in G and g^{-1} be the unique inverse. Then it follows that $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Proof of 1. Let $g \in G$ be arbitrary (we surpress the labels on the multiplication from here on)

$$\varphi(g) = \varphi(e_G * g) = \varphi(e_G) * \varphi(g)$$

Similarly on when multiplying e_G on the left of g. Thus $\varphi(e_G) = e_H$.

Proof of 2. Let $g \in G$ be arbitrary,

$$e_H = \varphi(e_G) = \varphi(g * g^{-1}) = \varphi(g) * \varphi(g^{-1})$$

and thus $\varphi(g^{-1})$ is the right inverse of $\varphi(g)$ and hence the inverse of $\varphi(g)$. $\square$

Definition: A bijective homomorphism $\varphi : G \to H$ is called an *isomorphism*. If such a map exist between two groups G, H we say G and H are *isomorphic* $G \cong H$.

Definition: The *kernel* of a homomorphism φ is the set of all elements in G that get mapped to the identity of H

$$\mathrm{Ker}(\varphi) = \{g \in G \big| \varphi(g) = e_H\}$$

One can check that this a subgroup of G but it is also a special kind of subgroup defined in the next section.

Proposition: $\varphi : G \to H$ is injective if and only if $\mathrm{Ker}(\varphi) = \{e_G\}$.

Proof: For the forward direction assume injectivity, and let $g \in \mathrm{Ker}(\varphi)$, then

$$\varphi(g) = e_H = \varphi(e_G)$$

but by injectivity this implies that $g = e_G$, hence $\mathrm{Ker}(\varphi) = \{e_G\}$.

For the backwards direction, let's assume $\mathrm{Ker}(\varphi) = \{e_G\}$. Let $g, h \in G$ be such that $\varphi(g) = \varphi(h)$, then

$$\begin{aligned} \varphi(g) &= \varphi(h) \\ \varphi(g)\varphi(h)^{-1} &= e_H \\ \varphi(gh^{-1}) &= e_H \end{aligned}$$

Which gives that $gh^{-1} \in \mathrm{Ker}(\varphi)$, but since $\mathrm{Ker}(\varphi)$ is trivial $gh^{-1} = e_H \implies g = h$, and hence φ is injective. $\square$

2. Normal Subgroups and Quotient Groups

A subgroup $H \leq G$ is called a normal subgroup if the following two sets are equal

$$gH = \{gh \big| h \in H\}$$

$$Hg = \{hg \big| h \in H\}$$

For any element $g \in G$. I.e H is normal if $gH = Hg \, \forall g \in G$. We denote this as $H \trianglelefteq G$. The sets gH and Hg are called *left/right cosets* respectively.

Note that $gH = Hg$, does not mean that $gh = hg$ for every element $h \in H$. But rather that the two are equal as sets meaning for any $h \in H$ there exists an $h' \in H$ such that $gh = h'g$. From this its also easy to see a different way to express this is that $ghg^{-1} = h'$, which means that $ghg^{-1} \in H$ for any element $h \in H$. So defining the following set

$$gHg^{-1} = \left\{ ghg^{-1} \middle| h \in H \right\}$$

Then we can see an equivalent characterization is that H is normal iff $gHg^{-1} \subseteq H$. This characterization is my preferred way of thinking of a Normal subgroup, what it means is that the subgroup H is invariant under the action of G. We will talk about this more in depth when we get to group actions.

Proposition: If $\varphi : G \longrightarrow H$ is a group homomorphism, then $\mathrm{Ker}(\varphi)$ is a normal subgroup of G.

Proof: Let $K = \mathrm{Ker}(\varphi)$ we would like to show this is a normal subgroup of G. We will show this by showing that $gHg^{-1} \subseteq H$. Take $k \in K$, by definition we have that $\varphi(k) = e_H$.

$$\begin{aligned} \varphi(gkg^{-1}) &= \varphi(g)\varphi(k)\varphi(g)^{-1} \\ &= \varphi(g)e_H\varphi(g)^{-1} \\ &= e_H \end{aligned}$$

so $gkg^{-1} \in K$, this implies that $gKg^{-1} \subseteq K$, $\forall g \in G$. Which shows that K is a normal subgroup. □

We can define an equivalence relation, by saying $g \sim g'$ iff $gH = g'H$. This is equivalent to saying that $g \sim g'$ iff $g^{-1}g' \in H$. One can check this satisfies all of the rules of a relation.

The coset gH is the equivalence class of the element g under the previous equivalence relation, meaning that only the element in gH are equivalent to g under the equivalence and no others.

Now as with sets we can define the quotient space, which is simply the set of all equivalence classes

$$G/H = \{gH \mid g \in G\}$$

We would like to equip this with a multiplication such that it also becomes a group of its own. As it turns out for this multiplication to be well defined H must be a normal subgroup of G. Let $H \trianglelefteq G$, we define the multiplication of cosets as follows

$$gH \, * kH = gkH$$

to show this is well defined, one has to check that the multiplication gives the same answer regardless of the representative of that class. It is easy to check that this holds if H is normal. Hence we can define the *quotient group* G/H, as the quotient space with the previous multiplication. Notice that the identity element of this group is $eH = H$.

3. Fundamental homomorphism theorem

Let $\varphi : G \to H$ be a surjective group homomorphism. As seen earlier $\mathrm{Ker}(\varphi)$ is a normal subgroup of G. This means we can construct the quotient group $G/\mathrm{Ker}(\varphi)$. Let $K = \mathrm{Ker}(\varphi)$, consider the following map

$$\begin{aligned} \tilde{\varphi} : G/K &\longrightarrow H \\ gK &\mapsto \varphi(g) \end{aligned}$$

One can easily check that this map is well-defined since φ maps K to the identity in H. Furthermore the kernel of the homomorphism is trivial, to see this let $gK \in \mathrm{Ker}(\tilde{\varphi})$ then

$$\tilde{\varphi}(gK) = e_H = \varphi(g)$$

this implies that $g \in K$, and hence $gK = K$. Therefore $\mathrm{Ker}(\tilde{\varphi}) = K$, is the trivial group since it only contains the identity element. By an earlier proposition this implies that φ is injective, but since φ is also surjective we get that φ is an isomorphism. Hence we have shown

Theorem (Fundamental Homomorphism): Let $\varphi : G \to H$ be a surjective group homomorphism. then

$$G/\mathrm{Ker}(\varphi) \cong H$$

In most cases people will refer to this as the first isomorphism theorem when reformulated as follows. If $\varphi : G \to H$ is a homomorphism it is easy to show that the image $\mathrm{Im}(\varphi)$ is a subgroup of H. Since every map is surjective onto it's image $\varphi : G \to \mathrm{Im}(\varphi)$ defined in the obvious is a surjective homomorphism. Applying the fundamental homomorphism theorem we have

$$G/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$$

This works for any homomorphism not necessarily surjective and is refered to as the first isomorphism theorem.