# Conjugation & Homomorphisms

Conor Rajan

Friday 18$^{\text{th}}$ June, 2021

## 1 Conjugation

The **conjugate** of an element $h \in G$ by $g \in G$ is defined as $ghg^{-1}$. So what does $ghg^{-1}$ really describe? One thing that we can immediately notice is:

$$(ghg^{-1})(gkg^{-1}) = ghkg^{-1}$$

All we have done here is basically renamed each element. Our element $h$ would usually act on $k$ to give $hk$, but instead we can have the conjugate of $h$ act on the conjugate of $k$ to give use the conjugate of $hk$. Effectively, the conjugate does the exact same thing, but acts on some permutation of the elements of $G$. To illustrate this point we can look at the familiar identity from IA Groups:

$$\sigma(a_1 a_2 a_3 \dots a_k)\sigma^{-1} = (\sigma(a_1)\sigma(a_2)\sigma(a_3)\dots\sigma(a_k))$$

Here, we have conjugated some element of $S_n$ by another permutation $\sigma$, and we have retrieved the exact same permutation but the labelling $\{a_i\}$ has been changed into $\{\sigma(a_i)\}$.

Another example of such a relabelling is the "change of basis formula" from Vectors and Matrices:

$$P^{-1}AP = A'$$

This describes the relation between two matrices $A$ and $A'$, which describe the same transformation, yet with repect to a different basis, i.e conjugation.

This concept will be important for us later.

# 2 Homomorphisms

In IA Groups, the following definition of a homomorphism is given:

**Definition** (Homomorphism)**.** A **homomorphism** is a function $\phi \colon G \to H$ between two groups $(G, \star_G)$ and $(H, \star_H)$, if for all $a, b \in G$, we have:

$$\phi(a \star_G b) = \phi(a) \star_H \phi(b).$$

Furthermore, we define the **kernel** and **image** of $\phi$ as

$$\operatorname{Ker}(\phi) = \{g \in G : \phi(g) = e_G\}, \; \operatorname{Im}(\phi) = \{\phi(g) : g \in G\}$$

In other words, if we compose two symmetries $a$ and $b$ in $G$ and map the resulting symmetry to $H$, we will get the same thing that we would have by mapping $a$ and $b$ into $H$ separately and composing them in $H$.

## 2.1 Equivalence classes

Which elements are mapped to the same thing? Note that

$$\begin{aligned} \phi(a) = \phi(b) &\iff \phi(b^{-1}a) = e \\ &\iff b^{-1}a \in \operatorname{Ker}(\phi) \\ &\iff a = bx \text{ for some } x \in \operatorname{Ker}(\phi) \end{aligned}$$

Therefore precisely $|\operatorname{Ker}(\phi)|$ things are sent to the same place as $a$ for any given $a \in G$.

It is quite natural to define an equivalence relation based on this. Define the equivalence relation $R$ on $G$ by $aRb$ if $\phi(a) = \phi(b)$. What is the equivalence class of $a$? Well we already answered this above. The equivalence class of $a$ is:

$$[a] = \{ax : x \in \operatorname{Ker}(\phi)\}$$

Consider the function $f : G/R \to H$ defined by $[a] \mapsto \phi(a)$. This is well defined since every element of a given equivalence class is mapped to the same thing in $H$. Furthermore, notice that this is actually a homomorphism. This is because:

$$f([a])f([b]) = \phi(a)\phi(b) = \phi(ab) = f([ab])$$

Furthermore, $f : G/R \to \operatorname{Im}(\phi)$ is actually a surjection. And wait! Its an injection too since each equivalence class must clearly be sent to different things by $\phi$. So we have an isomorphism:

$$f : G/R \to \operatorname{Im}(\phi)$$

The set $G/R$ of all the equivalence classes may also be viewed as a group, called the quotient group and is usually written $G/\operatorname{Ker}(\phi)$. Therefore we have just recovered the Isomorphism theorem.

## 2.2 Normal Subgroups

What happens when we conjugate an element of the kernel? Going back to how we thought of conjugation, the answer is simple. Conjugation is just a way of "renaming" symmetries, so when we conjugate a symmetry which is mapped to the trivial symmetry, it must still be mapped to the simple symmetry. This is because the trivial symmetry is trivial, no matter how you view it. More formally, if $g \in G, a \in \mathrm{Ker}(\phi)$:

$$\phi(gag^{-1}) = \phi(g)\phi(a)\phi(g^{-1}) = \phi(g)e\phi(g^{-1}) = e$$

This is a pretty special property when you think about it. Not only is such a subgroup closed under the group operation $\star$, but it is also "the same" regardless of how you view it. It is almost a stricter definition of a subgroup and in fact we will treat it as such.

**Proposition.** *Every normal subgroup is the kernel of some homomorphism and vice versa*

*Proof.* We have already seen that the kernel of every homomorphism is normal.

To see that each normal subgroup is a kernel of a homomorphism, we will construct a homomorphism explicitly. Given a subgroup $H \triangleleft G$, consider the equivalence relation $R$ on $G$ where $aRb$ if $a^{-1}b \in H$. Then we define the function $\theta : G \to G/R$ by $g \mapsto [g]$ where $[g]$ is the equivalence class of $g$ under $R$.

At this point $G/R$ is just a set as we have not defined a group operation on it. However, the normality of $H$ in $G$ will allow us to define a natural operation.

Define $\star : G/R \times G/R \to G/R$ by $[a] \star [b] \mapsto [ab]$. This is indeed well defined since if $[a_1] = [a_2]$ and $[b_1] = [b_2]$:

$$(a_2b_2)^{-1}(a_1b_1) = b_2^{-1}a_2^{-1}a_1b_1 = b_2^{-1}b_1b_1^{-1}h_1b_1 = b_2^{-1}b_2h_2 \in H \text{ for some } h_1, h_2 \in H$$

And so $[a_1b_1] = [a_2b_2]$. Now we can see that $\theta$ is indeed a homomorphism:

$$\theta(a) \star \theta(b) = [a] \star [b] = [ab] = \theta(ab)$$

And what is the kernel of $\theta$? Well clearly $[e]$ is the identity in $G/R$ so the kernel is just the elements $x$ such that $[x] = [e]$, or $e^{-1}x \in H$. Clearly these are exactly the elements of $H$, so $\mathrm{Ker}(\theta) = H$ as required.

$\square$

# 3 Conjugation as a Group Action

I mentioned previously that conjugation is effectively renaming each element of $G$ and so conjugation by $g \in G$ actually describes a permutation of the elements of $G$. We can formalise this by considering the map $\alpha : G \to \mathrm{Sym}(G)$ where each $g \in G$ is mapped to the corresponding permutation of $G$ it describes by conjugation.

It is quite simple to see that $\alpha$ is in fact a homomorphism.

$\alpha$ is actually a special type of homomorphism. For a set $X$ we call homomorphisms $\phi : G \to \mathrm{Sym}(X)$ **group actions** and say that $G$ **acts** on $X$. So since $X = G$ for $\alpha$, we say that $\alpha$ is an action of $G$ on itself.

What does the map $\alpha$ tell us about $G$? Well consider the kernel of $\alpha$.

$$\begin{aligned} x \in \mathrm{Ker}(\alpha) &\iff xgx^{-1} = g,\ \forall g \in G \\ &\iff x \in Z(G) \end{aligned}$$

So the kernel of $\alpha$ is precisely the centre of $G$. Hence if $G$ is abelian, $G = Z(G)$ and so $G/\mathrm{Ker}(\alpha) = \{e\} \cong \mathrm{Im}(\alpha)$ and so the image of alpha is precisely $G$.

A nice result about centres is

**Proposition.** *If $G$ is a group and $G/Z(G)$ is cyclic, $G$ is abelian.*

*Proof.* Suppose not. Then $\exists x \in G \setminus Z(G)$ such that $x$ generates $G/Z(G)$. Hence for any $g_1, g_2 \in G$ there exists $n, m \in \mathbb{Z}$ and $y, z \in Z(G)$ such that $g_1 = x^n y, g_2 = x^m z$. Hence

$$\begin{aligned} g_1 g_2 &= x^n y x^m z = x^n x^m y z \\ &= x^{n+m} z y = x^m x^n z y \\ &= x^m z x^n y = g_2 g_1 \end{aligned}$$

Since $g_1$ and $g_2$ were arbitrary, it follows that $G$ is abelian so $G = Z(G)$ and in fact $G/Z(G) = \{e\}$. $\square$

An immediate corollary of this is

**Corollary.** *There is no group $G$ with $|G : Z(G)| = p$ for $p \in \mathbb{Z}$ prime.*

*Proof.* If $Z(G)$ has prime index, then $G/Z(G) \cong C_p$ which is cyclic. But by the above theorem $G/Z(G) = \{e\}$ so this is a contradiction. $\square$