Core Algebra: Lecture 3, Homomorphisms and Normal Groups[1]

Definition 2.1. If G and H are groups, a **homomorphism (morphism)** $\phi : G \to H$ is a map $\phi : G \to H$ which preserves all structure, i.e.

1. $\forall\ g_1, g_2 \in G, \phi(g_1 g_2) = \phi(g_1)\phi(g_2)$
2. $\phi(e_G) = e_H$
3. $\phi(g^{-1}) = \phi(g)^{-1}$

Remark 2.2. Properties 2. and 3. follow from 1., hence need not be checked independently. Indeed, by 1.

$$\phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_G)$$

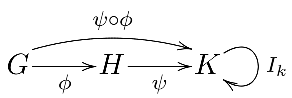
Cancelling $\phi(e_G)$ on both sides, we get that $\phi(e_G) = e_H$. Furthermore,

$$e_H = \phi(e_G) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1}) \Rightarrow \phi(g^{-1}) = (\phi(g))^{-1}$$

Another property: $\phi(g^n) = (\phi(g))^n$.

(Groups, morphisms) is an example of a "category":

1. Morphisms can be composed and the result of composition is morphisms back again.
2. Every object (group) has a distinguished "identity morphism".

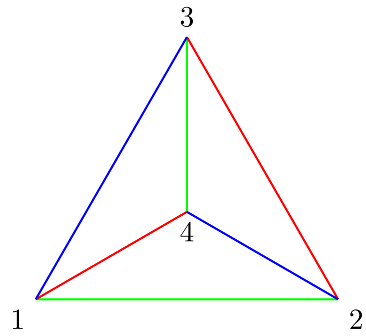


Examples

1. If V and W are vector spaces and $T : V \to W$ is a linear transformation, then $(V, +) \xrightarrow{T} (W, +)$ is a group morphism.
2. $(\mathbb{R}, +) \xrightarrow{exp} (\mathbb{R}_{>0}, +)$
   $x \longmapsto e^x$
3. For $H < G$ (i.e. H a subgroup of G), the inclusion $i_H : H \to G$ is a group morphism.
4. Given any $G, g \in G$, "conjugation by g" for $h \in G$: $h \longmapsto h^g := g^{-1}hg \in G$.
   Properties of conjugation:
   a) $(h_1h_2)^g = h_1^g h_2^g$ since $g^{-1}h_1h_2g = g^{-1}h_1gg^{-1}h_2g$
   $\Rightarrow$ conjugation is an endomorphism and $(h^n)^g = (h^g)^n$.
   b) $h^{(g_1g_2)} = (h^{g_1})^{g_2} \Rightarrow (h^g)^{g^{-1}} = h^{(gg^{-1})} = h^e = h$
   $\Rightarrow$ conjugation is an "automorphism".
   c) $(a^b)^c = (a^c)^{(b^c)}$

[1] Notes from Professor Bar-Natan's Fall 2010 Algebra I class. All the mistakes are mine, please let me know if you find any! (ivahal@math.toronto.edu)

5. $\phi : S_4 \twoheadrightarrow S_3$. ϕ is defined using the observation that $S_4 = Aut(\triangle)$, the group of automorphisms of the tetrahedron, and if we use three colours, say red (R), green (G), and blue (B) to colour the edges of the tetrahedron using the same colour on opposite edges, then any element of $Aut(\triangle)$ preserves opposite colouredness. On the other hand, $S_3 = S(R, G, B)$. So, for instance we have:



$$\begin{matrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 1 \end{matrix} \quad \xrightarrow{\phi} \quad \begin{matrix} R & G & B \\ \downarrow & \downarrow & \downarrow \\ G & R & B \end{matrix}$$

Claim 2.3. *If $\phi : G \to H$ is a morphism, then $ker\phi := \phi^{-1}(e_H) < G$ and $im\phi < H$.*

Moral: S_3 is an image of S_4.

Question: Is S_3 ($< S_4$) also $ker\phi$ for some $\phi : S_4 \to (?)$?

Remark 2.4. $\phi(h^g) = \phi(h)^{\phi(g)}$. So, if $h \in ker\phi$:

$$\phi(h^g) = \phi(h)^{\phi(g)} = e_H^{\phi(g)} = e_H \quad \Rightarrow \quad h^g \in ker\phi$$

Definition 2.5. $N < G$ is called **normal** if $\forall\, n \in N, g \in G,\ n^g = g^{-1}ng \in N$, denoted $N \triangleleft G$.

Claim 2.6. $(ker\phi) \triangleleft G$.

Now we can answer the earlier question by looking at: "$S_3 \triangleleft S_4$?":

$$[2\ 3\ 1\ 4]^{[1\ 2\ 4\ 3]} = [1\ 2\ 4\ 3]^{-1}[2\ 3\ 1\ 4][1\ 2\ 4\ 3] = [2\ 4\ 3\ 1] \notin S_3$$

So, S_3 is not normal in S_4 and hence there is not morphism from S_4 whose kernel is S_3.

Question: Given $N \triangleleft G$, is there a surjective morphism $\phi : G \twoheadrightarrow H$ s.t. $N = ker\phi$? Yes.

Set-theoretic aside

Consider $\phi : G \twoheadrightarrow H$ where ϕ is a function and G and H are sets.

An **equivalence relation** on X is a relation $x \sim y$ s.t.

1. $x \sim x$
2. $x \sim y \;\Rightarrow\; y \sim x$
3. $x \sim y,\ y \sim z \;\Rightarrow\; x \sim z$.

Then we have $X/\sim\, = \{[x]_\sim : x \in X\}$, $[x]_\sim = \{y : y \sim x\}$. X is thus decomposed into a disjoint union of equivalence classes. We also have:

$$\pi : X \twoheadrightarrow X/\sim, \quad x \mapsto [x]$$

If $\phi : X \to Y$ is a surjection, define $x_1 \sim x_2$ if $\phi(x_1) = \phi(x_2)$.

Question: If ϕ existed and $\sim$ was the corresponding equivalence relation, what properties would $\sim$ have?

$$\begin{aligned} g_1 \sim g_2 &\Leftrightarrow \phi(g_1) = \phi(g_2) \Leftrightarrow \phi(g_1)^{-1}\phi(g_2) = e_H \Leftrightarrow \phi(g_1^{-1}g_2) = e_H \\ &\Leftrightarrow g_1^{-1}g_2 \in N \Leftrightarrow g_1^{-1}g_2 = n \text{ for } n \in N \Leftrightarrow g_2 = g_1 n \text{ for } n \in N \\ &\Leftrightarrow g_2 \in g_1 N \end{aligned}$$

Claim 2.7. *If for $N < G$ we define $g_1 \sim g_2$ if $g_1^{-1}g_2 \in N \quad \Leftrightarrow \quad g_2 \in g_1 N$, then $\sim$ is an equivalence relation.*

Indeed, (checking transitivity) if $g_1 \sim g_2$ and $g_2 \sim g_3$ then $g_2 = g_1 n_1,\ g_3 = g_2 n_2$ and :

$$g_3 = g_2 n_2 = g_1 n_1 n_2 = g_1(n_1 n_2) \ \Rightarrow g_1 \sim g_3 \text{ since } n_1 n_2 \in N$$

So $G/\sim$ makes sense as a set:

$$\begin{aligned} \phi : G &\to G/\sim = G/N \\ g &\mapsto [g]_\sim = [g]_N = [g] \end{aligned}$$

What abour multiplication? Thought process:

$$[g_1]\,[g_2] = \phi(g_1)\phi(g_2) = \phi(g_1 g_2) = [g_1 g_2]$$

Definition 2.8. If $N \triangleleft G$, set $[g_1] \cdot [g_2] = [g_1 g_2]$.

Claim 2.9. *The above makes sense ($\cdot$ is "well-defined"), i.e. if $g_1' \sim g_1$ and $g_2' \sim g_2$ then $[g_1' g_2'] = [g_1 g_2]$ or in other words $g_1' g_2' \sim g_1 g_2$.*

Proof. We have $g_1' = g_1 n_1,\ g_2' = g_2 n_2$, so:

$$g_1' g_2' = g_1 n_1 g_2 n_2 = g_1 g_2 g_2^{-1} n_1 g_2 n_2 = g_1 g_2 n_1^{g_2} n_2 = g_1 g_2 n \text{ for some } n \in N$$

where the last step follows from normality. □

Theorem 2.10. *(**First Isomorphism Theorem**) Given $\phi : G \to H$, $G/ker\phi \cong im(\phi)$, i.e. there exists an invertible morphism $\psi : G/ker\phi \to im(\phi)$.*

Proof. Let $\psi : [g]_{ker\phi} \longmapsto \phi(g)$.
Exercise:

1. ψ is well-defined.
2. ψ is a morphism.
3. ψ is invertible.

□

Claim 2.11. *Given $N < G$, $\exists$ bijection $[g_1]_N \to [g_2]_N$ for any $g_1, g_2 \in G$.*

Proof. Use $g_1' \mapsto g_2 g_1^{-1} g_1'$ for any $g_1' \in [g_1]$. □

Hence, all equivalence classes $[g] = \{gn : \ n \in N\}$ have the same size $= |N|$ and so $|N| \mid |G|$.