

## Groups : homomorphisms

Suppose that we have two groups,  $(G, \bullet)$  and  $(H, \star)$ . Treating these just as sets, there would be many maps between them, as we could freely send things anywhere. However, a *homomorphism* attempts to preserve some structure: it ‘respects the group operation’. There is one rule for a homomorphism: that the map  $\theta : (G, \bullet) \rightarrow (H, \star)$  obeys

$$\boxed{\theta(g_1 \bullet g_2) = \theta(g_1) \star \theta(g_2).}$$

In other words, we must get the same result whether we multiply the elements of  $G$  before mapping them to  $H$ , or map them across individually and then multiply the results.

*Example.* We have met such a function before: the determinant obeys  $\det(AB) = (\det A)(\det B)$ , so it is a homomorphism from the group of ‘invertible matrices under matrix multiplication’ to the group of ‘non-zero real numbers under multiplication’.

1. In  $G$ , we have  $e_g = e_g \bullet e_g$ , and so in  $H$  we find  $\theta(e_g) = \theta(e_g \bullet e_g) = \theta(e_g) \star \theta(e_g)$ .

Then, inverting  $\theta(e_g)$  from both sides gives

$$\boxed{\theta(e_g) = e_h.}$$

*Example.*  $\det I = 1$ .

2. In  $G$ , we have  $g \bullet g^{-1} = e_g$ , so applying  $\theta$  gives  $\theta(g \bullet g^{-1}) = \theta(e_g)$ . Using our homomorphism rule and result 1 above gives  $\theta(g) \star \theta(g^{-1}) = e_h$ .

In other words, in  $H$ , the element which inverts  $\theta(g)$  is  $\theta(g^{-1})$ . That is

$$\boxed{\theta(g)^{-1} = \theta(g^{-1}).}$$

*Example.*  $\det(A^{-1}) = 1/\det A$ .

3. Applying our homomorphism rule repeatedly gives  $\theta(g^n) = \theta(g \bullet g^{n-1}) = \theta(g) \star \theta(g^{n-1}) = \dots$ , and so

$$\boxed{\theta(g^n) = \theta(g)^n.}$$

*Example.*  $\det(A^n) = (\det A)^n$ .

4. We begin with a lemma, which is a general result and nothing to do with homomorphisms.

*Lemma.* Let  $g \in G$  have order  $d$ . If  $g^k = e$ , then  $d$  divides  $k$ .

*Proof.* Write  $k = \lambda d + r$  where  $0 \leq r < d$ . Then

$$e = g^k = g^{\lambda d + r} = (g^d)^\lambda g^r = e^\lambda g^r = g^r$$

Since  $d$  is the smallest positive power to which we raise  $g$  and get  $e$ , but  $0 \leq r < d$ , we must have  $r = 0$ , and so  $k$  is a multiple of  $d$ . □

Now, let’s return to our homomorphism  $\theta : G \rightarrow H$ . Suppose that  $g \in G$  has order  $d$ . Then

$$e_h = \theta(e_g) = \theta(g^d) = \theta(g)^d$$

So by the lemma, in  $H$  we find that the order of  $\theta(g)$  divides  $d$ . In other words,

$$\boxed{\text{the order of } \theta(g) \text{ divides the order of } g.}$$

(Note that this implies that if  $\theta$  is an *isomorphism* then the order of  $g$  and  $\theta(g)$  are the same.)

*Example.* Let  $A_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$  and  $A_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ . Then both  $A_1$  and  $A_2$  have order 2, but  $\det A_1 = -1$  has order 2, while  $\det A_2 = 1$  has order 1.

*Example.* Groups, examples sheet 1, question 6 asks:

“Let  $C_n$  be the cyclic group with  $n$  elements and  $D_{2n}$  the group of symmetries of the regular  $n$ -gon. If  $n$  is odd and  $\theta : D_{2n} \rightarrow C_n$  is a homomorphism, show that  $\theta(g) = e$  for all  $g \in D_{2n}$ . What can you say if  $n$  is even? Find all the homomorphisms from  $C_n$  to  $C_m$ .”

Let's give things names:

$$D_{2n} = \langle a, b : a^n = b^2 = e_d, ba = a^{-1}b \rangle$$

$$C_n = \langle c : c^n = e_c \rangle$$

We don't yet know what  $\theta(a)$  and  $\theta(b)$  are. However, they live in  $C_n$ , which is a group of order  $n$ , so via Lagrange's Theorem, we know that the orders of  $\theta(a)$  and  $\theta(b)$  must divide  $n$ .

In  $D_{2n}$ , we have  $b^2 = e_d$ . Applying  $\theta$  and using our earlier results gives

$$e_c = \theta(e_d) = \theta(b^2) = \theta(b)^2$$

So, in  $C_n$ , we know that  $\theta(b)^2 = e_c$ . So the order of  $\theta(b)$  must divide 2: it is either an element of order 2, or it could already equal  $e_c$ .

We also know that  $a^n = e_d$ . Applying  $\theta$  here would tell us in a similar way that  $\theta(a)$  has order dividing  $n$ . But we already knew that via Lagrange, so that hasn't helped.

But we also know that in  $D_{2n}$ , we have  $ba = a^{-1}b$ . Applying  $\theta$  to this, and combining our earlier results gives

$$\theta(b)\theta(a) = \theta(ba) = \theta(a^{-1}b) = \theta(a)^{-1}\theta(b)$$

Now, we said earlier that  $\theta(b)$  was either of order 2 or was  $e_c$  itself. If it were  $e_c$ , then we could reduce this equation to just  $\theta(a) = \theta(a)^{-1}$ . But in fact, we can reach this conclusion without making any assumptions on the value of  $\theta(b)$ .

Since  $C_n$  is abelian, we can swap the terms on the left hand side, giving  $\theta(a)\theta(b) = \theta(a)^{-1}\theta(b)$ . Then we may simply invert  $\theta(b)$  from each side, giving  $\theta(a) = \theta(a)^{-1}$ .

Therefore, in  $C_n$ , we know that  $\theta(a)^2 = e_c$ . So, like  $\theta(b)$ , we know that  $\theta(a)$  has order dividing 2.

Recall the result from Lagrange: the order must also divide  $n$ . If  $n$  is odd, then the orders of  $\theta(a)$  and  $\theta(b)$  therefore divide both 2 and some odd number  $n$ , so both must equal 1. Thus if  $n$  is odd, we must have  $\theta(a) = \theta(b) = e_c$ . And since every element in  $D_{2n}$  may be written as a combination of  $a$  and  $b$ , we have that  $\theta(g) = e_c$  for all  $g \in D_{2n}$ , as required.

If  $n$  is even, then it is possible for  $\theta(a)$  or  $\theta(b)$  to have order 2, since  $C_n$  now has an element of order 2, namely  $c^{n/2}$ . We get four possible homomorphisms. (You should check that all four choices do actually work.)

Now have a go at the last bit, from  $C_n$  to  $C_m$ . Start by considering  $\theta(c^n)$  and work out the possible orders of  $\theta(c)$ .