11 Homomorphisms and Isomorphisms

We have already seen that it is possible for the same group to appear in more than one form. For example

$$G_1 = \{1, a, a^2, b, ab, a^2b\} \quad \text{where } a^3 = b^2 = 1,\ ab = ba$$

is a representation of the cyclic group

$$C_6 = \{1, x, x^2, x^3, x^4, x^5\} \quad \text{where } x^6 = 1$$

as every element can be generated by ab.

When two groups are really the same structurally we call them *isomorphic.* More formally we have the following definition:

Definition 11.1:

Two groups G(*) and G'(°) are said to be *isomorphic* if there is a one-one and onto mapping $\theta : G \to G'$ such that $(x*y)\theta = (x\theta)°(y\theta)$. (#)

θ is said to be an *isomorphism.* We indicate that the groups G and G' are isomorphic by writing $G \cong G'$.

Condition (#) is precisely what we need to ensure that the structures of G and G' are identical. We note that on the left hand side our operation is in G and we then apply θ to the result while on the right hand side we apply θ first and then combine the elements in G'. Normally the different operations will be clear to us and we will write (#) as $(xy)\theta = (x\theta)(y\theta)$.

Clearly two groups can only be isomorphic if they have the same number of elements as otherwise we can't find a one-one and onto function between them.

Returning to our example above we need to find a mapping from G_1 to C_6 that satisfies our isomorphism condition. Our approach for finding an isomorphism between groups G and G' is to follow the steps below:

1. Identify elements that will generate G. We have already seen that G_1 can be generated by ab or by a^2b. We will choose {ab} as our generating set.

2. Map the elements of our generating set onto elements in G' of the same order. In this case we map {ab} to the element x as both have order 6.

3. Use the property (#) to determine the mapping of the remaining elements.

   $(ab)^2 = a^2$. Hence $(a^2)\theta = (ab)^2\theta = ((ab)\theta)((ab)\theta) = xx = x^2$.
   $(ab)^3 = b$. Hence $(b)\theta = (ab)^3\theta = ((ab)\theta)^3 = x^3$
   $(ab)^4 = a$. Hence $(a)\theta = (ab)^4\theta = ((ab)\theta)^4 = x^4$
   $(ab)^5 = a^2b$. Hence $(a^2b)\theta = (ab)^5\theta = ((ab)\theta)^5 = x^5$

$(ab)^6 = 1$. Hence $1\theta = (ab)^6\theta = ((ab)\theta)^6 = x^6 = 1$.

4. Confirm that the defining relations of G are still relations in G'.

Here

$(ab)\theta = (a\theta)(b\theta) = x^4x^3 = x \quad (ba)\theta = (b\theta)(a\theta) = x^3x^4 = x$ so $(ab)\theta = (ba)\theta$
$(a^3)\theta = (a\theta)^3 = x^4x^4x^4 = 1 = 1\theta$
$(b^2)\theta = (b\theta)^2 = x^3x^3 = 1 = 1\theta$

and so relations in G_1 are still relations in C_6.

There are two things that can go wrong with this process (even if both groups have the same number of elements) - in both cases we have to assume that we have not found an isomorphism.

a) There may be no elements of the correct order in G' for us to map our generating elements onto. In this case G and G' cannot be isomorphic.

b) We may be able to find a mapping of generating elements that preserves order but inconsistencies may arise in the defining equations or the mapping may not be one-one. In this case we need to check if there are other possible mappings of the generating elements that might be suitable.

We illustrate the way in which things might go wrong with an example:

Example 11.1.2

Our library of groups tells us that D_4 and Q_4 are different groups. We consider whether we can find an isomorphism.

Step 1: $D_4 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$ where $a^4 = 1$, $b^2 = 1$, $ba = a^3b$. Thus we choose $\{a,b\}$ as our generating set. We note that a has order 4 while b has order 2.

Step 2: $Q_4 = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$ where $x^4 = 1$, $y^2 = x^2$, $yx = x^3y$ and so we have one element x^2 of order 2 and 6 elements of order 4. We therefore have a choice of mappings for a but b must be mapped to the element x^2. We choose

$$a \to x, \quad b \to x^2$$

as our trial mapping.

Step 3: If a is mapped to x then $a^2\theta = (a\theta)(a\theta) = x^2$.

But we already know that b is mapped to x^2 and so this mapping is not one-one. Hence it is not an isomorphism.

Exercises 11.1

1. In order to show that D_4 and Q_4 are not isomorphic we would have to try the other possible mappings of the generating elements:

   $a \to x^3$, $b \to x^2$
   $a \to y$, $b \to x^2$
   $a \to xy$, $b \to x^2$
   $a \to x^2y$, $b \to x^2$
   $a \to x^3y$, $b \to x^2$

   In each case show that an inconsistency occurs.

2. Try to find isomorphisms between the following pairs of groups:

   a) $G = \{1, a, b, ab, ba, aba\}$ where $a^2 = b^2 = 1$, $aba = bab$
   $G' = \{1, x, x^2, y, xy, x^2y\}$ where $x^3 = y^2 = 1$, $yx = x^2y$

   b) $G = \{1, a, a^2, a^3, b, ab, a^2b, a^3b, b^2, ab^2, a^2b^2, a^3b^2\}$, $a^4 = b^3 = 1$, $ba = ab$
   $G' = \{1, x, x^2, x^3, x^4, x^5, x^6, x^7, x^8, x^9, x^{10}, x^{11}\}$ where $x^{12} = 1$

   c) G of question a) and the permutation group S_3.

   d) C_4 and $Z_5 - \{[0]\}$ (with respect to multiplication of congruence classes).

   e) C_6 and $Z_7 - \{[0]\}$ (with respect to multiplication of congruence classes).

11.2 Other methods of determining if two groups are isomorphic

Sometimes the method described above may not be feasible (for example our groups may be infinite) and so we need to have other methods.

To show that G and G' are isomorphic we may be able to construct a mapping $\theta: G \to G'$ and show that $(xy)\theta = (x\theta)(y\theta)$ for every choice of x and y.

To show that G and G' are not isomorphic we need to find a structural property of one group that is not shared by the other. Possible structural properties might include:

G is abelian but G' is not

G is cyclic but G' is not

G has three elements of order 2 but G' does not

Example 11.2.1

We claim that the groups $\mathbf{R}(+)$ (the group of all real numbers wrt addition) and $\mathbf{R}^+-\{0\}(.)$ (the group of positive real numbers wrt multiplication) are isomorphic. This follows since consider the mapping θ from $\mathbf{R}$ to $\mathbf{R}^+-\{0\}$ given by $x\theta = e^x$. We claim this is one-one (since $e^x = e^y \Rightarrow x = y$) and onto (since if $x \in \mathbf{R}^+-\{0\}$ then x will be the image under θ of $ln(x)$).

Furthermore the function satisfies our property (#) since

$$(x+y)\theta = e^{x+y} = e^x e^y = (x\theta)(y\theta)$$

and so θ is an isomorphism.

Example 11.2.2

We claim that the group $\mathbf{R}-\{0\}(.)$ and $\mathbf{C}-\{0\}(.)$ (the groups of non-zero real and complex numbers respectively, wrt multiplication) are not isomorphic. There are a number of structural properties that we can use to show this. For instance

- $\mathbf{C}-\{0\}(.)$ has elements of order 4 (-i and +i) while $\mathbf{R}-\{0\}(.)$ doesn't.
- The equation $x^2 = a$ can always be solved in $\mathbf{C}$ but has no solutions in $\mathbf{R}$ if $a<0$.

11.3 Theorems about Isomorphism

Theorem 11.3.1

Let θ be an isomorphism between two groups $G(*)$ and $G'(\circ)$. Then

i) $1_G\theta = 1_{G'}$ (identity element must be mapped to the identity element)
ii) $(a^{-1})\theta = (a\theta)^{-1}$ (inverse elements get mapped to inverse elements)

Proof

i) $a * 1_G = a = 1_G * a$

Hence

$$(a * 1_G)\theta = a\theta = (1_G * a)\theta$$
$$\Rightarrow \quad a\theta \circ 1_G\theta = a\theta = 1_G\theta \circ a\theta$$

But then $1_G\theta$ acts as an identity element in G'. Since we have seen that there is only one identity element it follows that $1_G\theta = 1_{G'}$.

ii) $a * a^{-1} = 1_G = a^{-1} * a$

Hence

$$(a * a^{-1})\theta = 1_G\theta = (a^{-1} * a)\theta$$
$$\Rightarrow \quad a\theta \circ a^{-1}\theta = 1_G\theta = 1_{G'} = a^{-1}\theta \circ a\theta$$

Hence $a^{-1}\theta$ is the inverse of $a\theta$ in G' as it is the thing we need to multiply $a\theta$ by to obtain $1_{G'}$. Hence $a^{-1}\theta = (a\theta)^{-1}$.

•

Theorem 11.3.2

If $\theta : G \to G'$ is an isomorphism then order(a) = order $(a\theta)$ for every a in G.

Proof

Suppose a has order n and $a\theta$ has order m.

1. $a^n = 1_G$. Thus $(a\theta)^n = a^n\theta = 1_G\theta = 1_{G'}$.

   Hence by theorems on the orders of elements n must be a multiple of m .

2. $(a^m)\theta = (a\theta)^m = 1_{G'}$. But θ is one-one and we know that $1_G\theta = 1_{G'}$. Hence

   $a^m = 1_G$. But again we must have that m is a multiple of n.

Hence m divides n and n divides m. Since m and n are both positive integers it follows that m = n.

•