Fundamentals of Pure Mathematics
Workshop 3 (Week 5): Homomorphisms and Isomorphisms

The point of this workshop is to practice working with homomorphisms, and to gain some intuition for when two groups are isomorphic.

> Let G, H be groups. Recall that we call a function $\theta\colon G \to H$ a *group homomorphism* if $\theta(g_1 g_2) = \theta(g_1)\theta(g_2)$ for all $g_1, g_2 \in G$. A group homomorphism that is also a bijection is called a *group isomorphism*, and in this case we write $G \cong H$.

Group homomorphisms are the way to transfer information from one group to another.

Question 1. Are the following group homomorphisms?

(a) $\mathbb{Z} \to \mathbb{Z}_n$ sending $z \mapsto z \bmod n$.

(b) $\mathbb{Z}_n \to \mathbb{Z}$ sending z (with $0 \leq z \leq n-1$) $\mapsto z$.

(c) $\mathbb{Z} \to \mathbb{Q}$ sending $z \mapsto \frac{z}{1}$.

(d) $\mathbb{Z}_n \to D_n$ sending $z \bmod n \mapsto g^z$ where g is rotation by an n^{th} of a turn.

Now for an arbitrary homomorphism $\theta\colon G \to H$ to be an isomorphism requires θ to be both injective and surjective.

Question 2. Let $\theta\colon G \to H$ be a group homomorphism.

(a) Show that θ is injective if and only if $\operatorname{Ker}\theta = \{e\}$.

(b) If θ is injective, show that $G \cong \operatorname{Im}\theta \leq H$.

Hence by (b), injective group homomorphisms allow us to view G as (isomorphic to) a subgroup of H.

When faced with determining whether two groups are the same (=isomorphic), unless you have good reasons to believe that they are, you should be very skeptical.

Question 3. Are the following groups isomorphic?

(a) $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(b) $\mathbb{Z}_{12}$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

(c) $\mathbb{Z}_{12}$ and $\mathbb{Z}_4 \times \mathbb{Z}_3$.

(d) S_3 and D_3.

(e) S_4 and D_4.

On the other hand, isomorphisms can appear quite often. The following shows that there can often be many incarnations of the same group, so being able to identify them as 'the same' is important.

Question 4. This question will give you lots of examples of isomorphisms.

(a) Show that the set

$$S_1 := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R}, \text{ not both zero} \right\}$$

is a group under multiplication of matrices. Do you recognise this group?

(b) Show that $S_1 \cong \mathbb{C}^*$, where recall $\mathbb{C}^*$ is the non-zero complex numbers considered as a group under multiplication.

(c) Find 2015 different 2×2 matrices M_i $(1 \leq i \leq 2015)$ such that $M_i^2 = -\mathbb{I}$.

(d) By using your solutions to (b) and (c), produce groups S_i $(1 \leq i \leq 2015)$ such that each $S_i \cong \mathbb{C}^*$.

In (d) you have produced 2015 groups S_i, each of which is isomorphic to $\mathbb{C}^*$. Thus from the viewpoint of group theory, all the groups S_i are the same.

In Q4 the groups were infinite, but finite groups also often appear as subgroups of matrices. Identifying them might not be so easy:

Question 5. Is the following subset of $\mathrm{GL}(2, \mathbb{C})$ a group, and if so to which familiar group is it isomorphic?

$$G := \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^2 \end{pmatrix}, \begin{pmatrix} \varepsilon^2 & 0 \\ 0 & \varepsilon \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \varepsilon \\ \varepsilon^2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \varepsilon^2 \\ \varepsilon & 0 \end{pmatrix} \right\}$$

where $\varepsilon := e^{\frac{2\pi i}{3}}$.

Solutions.

1. In each case, denote the rule by θ.
   (a) Yes. $\theta(z_1+z_2) := z_1+z_2 \bmod n = \theta(z_1)+\theta(z_2)$ for all $z_1, z_2 \in \mathbb{Z}$.
   (b) No. On one hand $\theta(1+(n-1)) = \theta(0_{\mathbb{Z}_n}) := 0_{\mathbb{Z}}$, but on the other $\theta(1)+\theta(n-1) = 1+(n-1) = n \neq 0_{\mathbb{Z}}$.
   (c) Yes. $\theta(z_1+z_2) := \frac{z_1+z_2}{1} = \frac{z_1}{1}+\frac{z_2}{1} = \theta(z_1)+\theta(z_2)$ for all $z_1, z_2 \in \mathbb{Z}$.
   (d) Yes. $\theta(z_1+z_2) := g^{z_1+z_2 \bmod n}$. Since $g^n = e$, we know that $g^{z_1+z_2 \bmod n} = g^{z_1+z_2}$. Hence
   $$\theta(z_1+z_2) := g^{z_1+z_2 \bmod n} = g^{z_1+z_2} = g^{z_1}g^{z_2} = \theta(z_1)\theta(z_2)$$
   for all $z_1, z_2 \in \mathbb{Z}_n$.

2. (a) Since $\theta(e) = e$ (by lectures), $\{e\} \subseteq \operatorname{Ker}\theta$. Now
   ($\Rightarrow$) Suppose that θ is injective. Let $g \in \operatorname{Ker}\theta$, then $\theta(g) = e = \theta(e)$ and so $g = e$. Hence $\operatorname{Ker}\theta \subseteq \{e\}$ and so $\operatorname{Ker}\theta = \{e\}$.
   ($\Leftarrow$) Suppose that $\operatorname{Ker}\theta = \{e\}$. Let $g_1, g_2 \in G$ be such that $\theta(g_1) = \theta(g_2)$, then since $\theta(g_1)^{-1} = \theta(g_1^{-1})$ (by lectures),
   $$e = \theta(g_1)^{-1}\theta(g_1) = \theta(g_1)^{-1}\theta(g_2) = \theta(g_1^{-1})\theta(g_2) = \theta(g_1^{-1}g_2)$$
   and so $g_1^{-1}g_2 \in \operatorname{Ker}\theta$. Hence $g_1^{-1}g_2 = e$ and so $g_1 = g_2$.
   (b) We first show that $\operatorname{Im}\theta$ is a subgroup of G, using the subgroup test. Since $e_H = \theta(e_G) \in \operatorname{Im}\theta$, therefore $\operatorname{Im}\theta \neq \emptyset$. Now let $h_1 = \theta(g_1)$ and $h_2 = \theta(g_2)$ be elements of $\operatorname{Im}\theta$. Then $h_1h_2 = \theta(g_1)\theta(g_2) = \theta(g_1g_2)$, so $h_1h_2 \in \operatorname{Im}\theta$. And $h_1^{-1} = \theta(g_1)^{-1} = \theta(g_1^{-1}) \in \operatorname{Im}\theta$. Thus by the subgroup test $\operatorname{Im}\theta \leq H$.
   Clearly $\theta : G \to H$ is surjective onto its image $\operatorname{Im}\theta$.
   Thus, since θ is injective, $\theta : G \to \operatorname{Im}\theta$ taking $g \mapsto \theta(g)$ is a bijective group homomorphism, i.e. a group isomorphism.

3. (a) No. $\mathbb{Z}_2 \times \mathbb{Z}_2$ has no element of order 4, whereas $\mathbb{Z}_4$ does.
   (b) No. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ has no element of order 12, whereas $\mathbb{Z}_{12}$ does.
   (c) Yes. Since $\gcd(4,3) = 1$, $\mathbb{Z}_4 \times \mathbb{Z}_3$ has an element of order 12, hence it is cyclic. All cyclic groups of a given order are isomorphic.
   (d) **Solution 1.** Yes. A symmetry of a graph is a bijection $V \to V$ where V is the set of vertices. Hence every element of D_3 gives a permutation of the vertices $\{1,2,3\}$ and so simply map $\theta\colon D_3 \to S_3$ sending $f \mapsto f$. This is clearly a group homomorphism (the operation on both sides is just composition of functions). Now if $f \in \operatorname{Ker}\theta$ then $\theta(f) = e$, so $f = e$. This shows that $\operatorname{Ker}\theta = \{e\}$ so θ is injective. Since both sets have size six, θ is also surjective. Hence θ is a group isomorphism.
   Solution 2. Yes. All non-abelian groups of order six are isomorphic (we will cover this later, see Jordan–Jordan §17 Theorem 3), so in particular $D_3 \cong S_3$.
   Solution 3. (this needs group actions) Yes. D_3 acts faithfully on the set $X := \{1,2,3\}$ of vertices of the 3-gon. This gives an injective group

homomorphism $D_3 \to S_{|X|} = S_3$. Since $|S_3| = 3! = 6 = 2 \times 3 = |D_3|$, this is also surjective, and so a group isomorphism.

(e) No. S_4 has order $4! = 24$, where D_4 has order $2 \times 4 = 8$.

(f) Yes. Both groups have order two, and there is only one group of order two (namely the cyclic group of order two).

4. (a) Use the test for a subgroup. Clearly S_1 is not empty. Further, if

$$\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} \in S_1$$

then

$$\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 - b_1b_2 & a_1b_2 + a_2b_1 \\ -(a_1b_2 + a_2b_1) & a_1a_2 - b_1b_2 \end{pmatrix}$$

which is still a member of S_1. Hence S_1 is closed. Finally, you can check that the inverse of

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in S_1$$

is

$$\frac{1}{a^2 + b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

which also belongs to S_1. This shows that S_1 is a subgroup of $\mathrm{GL}(2, \mathbb{R})$.

(b) Map $\theta \colon \mathbb{C}^* \to S_1$ by sending

$$x + iy \mapsto \begin{pmatrix} x & y \\ -y & x \end{pmatrix}.$$

Since $x + iy \in \mathbb{C}^*$, x and y cannot both be zero and so this is indeed a map. It is easy to check that θ is both injective and surjective, hence a bijective map. Finally

$$\begin{aligned} \theta((x_1 + iy_1)(x_2 + iy_2)) &= \theta(x_1x_2 - y_1y_2 + i(x_1y_2 + x_2y_1)) \\ &= \begin{pmatrix} x_1x_2 - y_1y_2 & x_1y_2 + x_2y_1 \\ -(x_1y_2 + x_2y_1) & x_1x_2 - y_1y_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{pmatrix} \begin{pmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{pmatrix} \\ &= \theta(x_1 + iy_1)\theta(x_2 + iy_2) \end{aligned}$$

and so θ is a group homomorphism.

(c) The observation is that in (a),

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

We can replace the matrix $M_1 := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ by *any* matrix M_i such that $M_i^2 = -\mathbb{I}$, and the proofs in (a) and (b) will still work. One way to produce such M_i is just to take the matrix M_1, multiply on the left by an invertible matrix T, and multiply on the right by T^{-1} (you can check that TM_1T^{-1} squares to $-\mathbb{I}$). For any $d \in \mathbb{R}$, consider

$$T := \begin{pmatrix} 1 & 1 \\ 1 & d \end{pmatrix}$$

(with $d \neq 1$ so that $\det T \neq 0$, so T is invertible). Then

$$T^{-1} = \frac{1}{d-1}\begin{pmatrix} d & -1 \\ -1 & 1 \end{pmatrix}$$

and

$$TM_1T^{-1} = \frac{1}{d-1}\begin{pmatrix} -(1+d) & 2 \\ -(1+d^2) & 1+d \end{pmatrix}$$

By varying d, we get the required matrices M_i (in fact, we can get infinitely many).

(d) Similarly to (a) and (b), the set $S_i := \{a\mathbb{I}+bM_i \mid a, b \in \mathbb{R},\ \text{not both zero}\}$ is a group, and the natural map $\mathbb{C}^* \to S_i$ sending $x + iy \mapsto x\mathbb{I} + yM_i$ is a group isomorphism.

5. **Solution 1.** It is a group (just use the test for a subgroup). If we set

$$a := \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^2 \end{pmatrix} \quad \text{and} \quad b := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

then observe that the elements in G are simply

$$\{e, a, a^2, b, ab, a^2b\}$$

which suggests that G is the dihedral group D_3. This can be shown directly (but is quite painful) — just consider the function $G \to D_3$ that sends a^ib^j ($0 \leq i \leq 2$, $0 \leq j \leq 1$) to g^ih^j where, as usual, g is the $\frac{1}{3}$rd turn rotation, and h is a reflection. This is clearly a bijection, and you can check (by exhausting all possibilities) that it is a group homomorphism.

Solution 2: G is a group (again by the test for a subgroup) which by inspection has six elements. Since $ab \neq ba$, it is non-abelian. All non-abelian groups of order 6 are isomorphic to D_3 (we will cover this later in the course, see Jordan–Jordan §17 Theorem 3), so in particular our group G is isomorphic to D_3.