Homework Assignment 3: Solutions

1. We begin by establishing important basic facts about group homomorphisms that we will use repeatedly throughout the course. Let G, H, K be groups, and let $\varphi : G \to H$ and $\psi : H \to K$ a homomorphisms.

(a) Show that $\varphi(1_G) = 1_H$.

Proof. Fix $g \in G$ and let $h = \varphi(g)$. Notice that:

$$\varphi(1_G) \cdot h = \varphi(1_G)\varphi(g) = \varphi(1_G \cdot g) = \varphi(g) = h.$$

Mutliplying both sides on the right by h^{-1} we get $\varphi(1_G) = 1_H$ as desired. □

(b) Show that $\varphi(x^{-1}) = \varphi(x)^{-1}$ for all $x \in G$.

Proof. Notice that

$$\varphi(x^{-1})\varphi(x) = \varphi(x^{-1}x) = \varphi(1_G) = 1_H.$$

Therefore by HW2 7(a) we are done. □

(c) Show that if $g \in G$ has finite order, then $|\varphi(g)|$ divides $|g|$.

Proof. Let $m = |g|$ and $n = |\varphi(g)|$. Then

$$\varphi(g)^m = \varphi(g^m) = \varphi(1_G) = 1_H.$$

Applying HW2 8(c), we are done. (Explicitly, that problem shows that $m \equiv n \mod n$, which means $n|m$ as desired.) □

(d) Show that if φ is an isomorphism, then so is φ^{-1}.

Proof. We already know that φ^{-1} is bijective since it is the inverse to a bijection. Therefore we must show that φ^{-1} is a homomorphism. Fix $x, y \in H$. Then $x = \varphi(a)$ and $y = \varphi(b)$ as φ is bijective. Therefore:

$$\varphi^{-1}(xy) = \varphi^{-1}(\varphi(a)\varphi(b)) = \varphi^{-1}(\varphi(ab)) = ab = \varphi^{-1}(x)\varphi^{-1}(y).$$

Therefore φ^{-1} is a homomorphism. □

(e) Show that if φ is an isomorphism, $|\varphi(g)| = |g|$.

Proof. There are two cases. First assume $|g| = \infty$. If $\varphi(g)^n = 1$ then

$$1 = \varphi^{-1}(1) = \varphi^{-1}(\varphi(g)^n) = \varphi^{-1}(\varphi(g^n)) = g^n,$$

a contradiction as g has infinite order. So therefore $|\varphi(g)| = \infty$ also.
Otherwise $|g| = n < \infty$. Then $|\varphi(g)| = m$ and $m|n$ by part (c). But by part (d) we can apply part (c) to φ^{-1} and see also that $n|m$. Therefore $n = m$. □

(f) Show that the composition $\psi \circ \varphi : G \to K$ is a homomorphism.

Proof. Let $x, y \in G$. Using that ψ and φ are homomorphisms we directly compute:

$$\psi(\varphi(xy)) = \psi(\varphi(x)\varphi(y)) = \psi(\varphi(x))\psi(\varphi(y))$$

as desired. □

(g) Suppose φ and ψ are both isomorphisms. Show that the composition $\psi \circ \varphi$ is as well.

Proof. We know the composition is a homomorphism by part (f). Furthermore, the composition of bijective functions is bijective (as in HW2 5), so we win. □

(h) Conclude that the relation *is isomorphic to* is an equivalence relation on the set of all groups.

Proof. Notice that $id_G : G \to G$ is a bijective homomorphism, so that $G \cong G$, proving reflexivity. If $G \cong H$, then there is an isomorphism $\varphi : G \to H$. By part (d) φ^{-1} is an isomorphism too so $H \cong G$ proving symmetry. Finally, if $\varphi : G \cong H$ and $\psi : H \cong K$, then by part (g) $\psi \circ \phi : G \cong K$, proving transitivity. □

2. Given a homomorphism $\varphi : G \to H$, we obtain 2 important subgroups, one of G and one of H. They are called the *kernel of* φ and *image of* φ and are defined by the following rules:

$$\begin{aligned} \ker \varphi &= \{g \in G : \varphi(g) = 1_H\}, \\ \operatorname{im} \varphi &= \{h \in H : h = \varphi(g) \text{ for some } g \in G\}. \end{aligned}$$

(a) Show that $\ker \varphi$ is a subgroup of G.

Proof. We know $1_G \in \ker \varphi$ by 1(a) so that it is nonempty. If $x \in \ker \varphi$ then applying 1(b) we have:

$$\varphi(x^{-1}) = \varphi(x)^{-1} = 1_H^{-1} = 1_H.$$

so that $x^{-1} \in \ker \varphi$ also. If $x, y \in \ker \varphi$, then

$$\varphi(xy) = \varphi(x)\varphi(y) = 1_H \cdot 1_H = 1_H,$$

so that xy is too. Thus it is a subgroup. □

(b) Show that $\operatorname{im} \varphi$ is a subgroup of H.

Proof. We must first show it is nonempty, but by 1(a) it contains 1_H. Next we show it contains inverses, but this follows by 1(b) as if $x = \varphi(a) \in \operatorname{im} \varphi$ then $x^{-1} = \varphi(a)^{-1} = \varphi(a^{-1})$. Finally, if $x = \varphi(a)$ and $y = \varphi(b)$ are in the image, then $xy = \varphi(a)\varphi(b) = \varphi(ab)$ is in the image as well. □

(c) *Important:* Show that φ is injective if and only if $\ker \varphi = \{1_G\}$. (This is an incredibly useful fact!)

Proof. Suppose φ is injective. If $g \in \ker\varphi$ then $\varphi(g) = 1_H = \varphi(1_G)$ so that by injectivity $g = 1_G$.
Conversely, suppose $\ker\varphi = \{1_G\}$. Fix $x, y \in G$ and suppose $\varphi(x) = \varphi(y) = h$. Then:

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = h \cdot h^{-1} = 1_H.$$

Thus $xy^{-1} = 1_G$. Multiplying on the right by y shows $x = y$ and so φ injects. □

3. The kernel has the following important generalization. For $h \in H$ define the *fiber over h* as

$$\varphi^{-1}(h) = \{g \in G : \varphi(g) = h\}.$$

This is sometimes also called the *preimage of h*. Observe that by definition, the kernel of φ is the fiber over 1.

(a) Show that the fiber over h is a subgroup if and only if $h = 1_H$.

Proof. If $h = 1_H$ then $\varphi^{-1}(h) = \ker\varphi$ which we showed was a subgroup in 2(a).
Conversely, suppose $\varphi^{-1}(h)$ is a subgroup. Then in particular it contains 1_G. So that $h = \varphi(1_G) = 1_H$ as desired. □

(b) Show that the *nonempty* fibers of φ form a partition of G. (In particular, if φ is surjective its fibers partition G.)

Proof. First notice we are only considering nonempty fibers so the elements of the partition are by definition nonempty. We must show their union is all of G, but if $g \in G$ then $\varphi(g) = h$ and so $g \in \varphi^{-1}(h)$ as desired. Lastly we must show they have empty intersections. Let $g \in \varphi^{-1}(h) \cap \varphi^{-1}(h')$. Then $h = \varphi(g) = h'$ so they were the same fibers to begin with. □

(c) Show that all nonempty fibers have the same cardinality. (Hint: if $\varphi^{-1}(h)$ is nonempty, build a bijection between it and $\ker\varphi$.) Observe that this generalizes 2(c).

Proof. (Note: in my opinion this is the most difficult problem of the assignment).
It suffices to build a bijection $f : \ker\varphi \to \varphi^{-1}(h)$. Fix some $x \in \varphi^{-1}(h)$. For $g \in \ker\varphi$, define $f(g) = x \cdot g$. Let us begin by first checking that this defines a map to $\varphi^{-1}(h)$, i.e., that the image of f actually lies in the fiber over h. To check this we apply φ to xg and notice that

$$\varphi(xg) = \varphi(x)\varphi(g) = h \cdot 1_H = h,$$

so that $xg \in \varphi^{-1}(h)$ as desired. What remains is to show that f is a bijection. To do this we construct an inverse $f^{-1} : \varphi^{-1}(h) \to \ker\varphi$. As f was multiplication by x then the inverse should be multiplication by x^{-1}. As above, we begin by showing this map actually lands in the kernel, that is, fixing $g' \in \varphi^{-1}(h)$, we must see that $x^{-1}g' \in \ker\varphi$. Applying φ we see

$$\varphi(x^{-1}g') = \varphi(x^{-1})\varphi(g') = \varphi(x)^{-1}\varphi(g') = h^{-1}h = 1_H,$$

so that it is indeed in the kernel. From here it is clear that f^{-1} is an inverse to f, as composition is multiplictation by $x^{-1}x$ or xx^{-1}, i.e., mutliplication by 1_G or the identity map. Thus we have built a bijection between $\ker\varphi$ and $\varphi^{-1}(h)$ and so they must have the same cardinality. □

4. Recall that we defined the kernel of a group action in class. Let's justify our terminology. Let $G \times A \to A$ be an action of G on a set A and let $\varphi : G \to S_A$ be the associated permutation representation.

   (a) Show that the kernel of the group action is equal to $\ker \varphi$.

   Proof. Let g be in the kernel of the group action, and consider $\varphi(g) = \sigma_g \in S_A$. Then for every $a \in A$ we have $\sigma_g(a) = g \cdot a = a$ as g acts trivially on every element in A. Thus $\sigma_g = id_A$ which is the identity element S_A. In particular, $\varphi(g) = 1$ and so $g \in \ker \varphi$. This shows that the kernel of the group action is contained in $\ker \varphi$.

   To show the reverse containment, fix some $g \in \ker \varphi$. We must show it acts trivially on every element of A, so fix some $a \in A$. Then

   $$g \cdot a = \sigma_g(a) = \varphi(g)(a) = id_A(a) = a$$

   so g is in the kernel of the action as desired. □

   (b) Show that the action is faithful if and only if the φ is injective. (Hint: Use 2(c).)

   Proof. The action is faithful if and only if the only element of the kernel is 1_G. By part (a) this says $\ker \varphi = \{1_G\}$, which by 2(c) is equivalent to φ being injective. □

5. We've seen that there is a relationship between the dihedral and symmetric groups. Let's explore this a bit.

   (a) Describe an injective homomorphism from $\varphi : D_{2n} \to S_n$ (you may describe this in words, but make sure to justify injectivity).

   Proof. Label the vertices of the n-gon $\{1, 2, \cdots, n\}$. Then applying a symmetry α give a permutation σ_α of these vertices, thus an element of S_n. This is a well defined function, and it is a homomorphism because composing two symmetries will compose the permutations of the vertices, and multiplication on both sides is exactly composition of functions.

   To observe injectivity we leverage 2(c). In particular, we notice that a symmetry is in the kernel precisely when it fixes all the vertices. But only the trivial symmetry does this, so the kernel of φ is trivial. □

   (b) In the map you described, what is the cycle decomposition of $\varphi(r)$ (where as usual r is the generator corresponding to clockwise rotation of the n-gon by $2\pi/n$)?

   Proof. Consider the rotation r. What permutation does it induce? Well, it sends 1 to 2, 2 to 3, 3 to 4, $\cdots$, $n-1$ to n, and n to 1. But this is precisely the n-cycle $(1\ 2\ 3 \cdots n-1\ n)$. □

   (c) Prove that $D_6 \cong S_3$.

   Proof. We have described an injective homomorphism $D_6 \to S_3$. But both D_6 and S_3 have order 6, so that by HW1 Problem 5 it must be bijective. □

6. In this exercise we show that you can compute the order of a permutation from its cycle decomposition.

   (a) Let G be a group. Two elements $x, y \in G$ are called *commuting elements* if $xy = yx$. Show that if x and y are commuting elements, then $(xy)^n = x^n y^n$.

   Proof. We first show the following identity. If x, y commute, then $x^n y = yx^n$. We proceed by induction on n. If $n = 1$, it is trivial. Now suppose the identity holds for n, we show it does for $n + 1$. Indeed:

   $$x^{n+1}y = x^n xy = x^n yx = yx^n x = yx^{n+1}.$$

   We now prove the main result. Again we proceed by induction. For $n = 1$ it is trivial. Suppose the identity holds for n. We show it does for $n+1$. Indeed, applying the above identity we see:

   $$(xy)^{n+1} = (xy^n)xy = x^n y^n xy = x^n xy^n y = x^{n+1}y^{n+1}.$$

   □

   (b) Give a counterexample to part (a) if the chosen elements do not commute.

   Proof. These are plentiful. We will consider $r, s \in D_{2n}$ for $n \geq 3$. Then $(sr)^2 = 1$ by HW2 9(e). But $s^2r^2 = r^2 \neq 1$. □

   (c) Let $\sigma = (a_1, a_2, \cdots, a_r) \in S_n$ be an r-cycle. Show that $|\sigma| = r$.

   Proof. We first show that $|\sigma| \geq r$. Indeed, let $1 \leq k < r$. Then $\sigma^k(a_1) = a_k$ so that σ^k cannot be the identity. It therefore suffices to show that $\sigma^r = 1$. Fix some $b \in \{1, \cdots, n\}$. If $b \neq a_k$ then certainly $\sigma^r(b) = b$ (indeed, $\sigma(b) = b$). Otherwise, $b = a_k$ for some k. Since:

   $$(a_1, a_2, \cdots, a_r) = (a_k, a_{k+1}, \cdots, a_r, a_1, a_2, \cdots, a_{k-2}, a_{k-1}),$$

   we may assume by relabelling that $k = 1$. But then certainly $\sigma^r(a_1) = a_1$. □

   (d) Prove that the order of a permutation is the least common multiple of the lengths of the cycles in its cycle decomposition. (Hint: You may freely use that disjoint cycles are commuting elements. You may find it useful to establish that the product of nontrivial disjoint cycles is never 1).

   Proof. We first establish the fact suggested in the hint. Suppose we consider the product of disjoint nontrivial cycles:

   $$\sigma = (a_1, \cdots, a_{n_a})(b_1, \cdots, b_{n_b}) \cdots (z_1, \cdots, z_{n_z}).$$

   Since theye are disjoint and nontrivial, we see that $\sigma(a_1) = a_2$ so that σ is not the identity.

   Now suppose $\sigma = \sigma_1\sigma_2 \cdots \sigma_r$ the cycle decomposition, and the length of each $\sigma_i = \ell_i$. Let m be the least common multiple of the ℓ_i. Then (for example by HW2 8(c)), we know that $\sigma_i^m = 1$ for all i, so that applying part (a) we conclude that $\sigma^m = 1$. Therefore $|\sigma| \leq m$. To conlcude, suppose $n < m$. Then there is some i such that $\ell_i \not| n$ (since m

is the least common multiple and n is smaller). Again by HW2 8(c), this implies that $\sigma_i^n \neq 1$. So:

$$\sigma^n = \sigma_1^n \sigma_2^n \cdots \sigma_r^n,$$

is the product of disjoint cycles, at least one of which is nontrivial. Therefore it cannot be 1. (We point out that σ_i^n need not be a single cycle, for example, $(1,2,3,4)^2 = (1,3)(2,4)$, but the cycles making up σ_i^n will still be disjoint from those making up σ_j^n). □

7. We hinted in class that if A and B are sets of the same cardinality, then their permutation groups S_A and S_B (defined in HW2#5) are isomorphic. Let's prove it. To begin, fix a bijective function $\theta : A \to B$.

   (a) Let $f : A \to A$ be bijective. Show that $\theta \circ f \circ \theta^{-1} : B \to B$ is bijective. (Hint: what is its inverse?)

   Proof. As in HW2 5 we know that the composition of bijective functions is bijective. Since θ, f, θ^{-1} are all bijective, so is their composition. □

   (b) Part (a) allows us to construct the following function:

$$\begin{array}{ccc} S_A & \xrightarrow{\varphi} & S_B \\ f & \longmapsto & \theta \circ f \circ \theta^{-1}. \end{array}$$

   Show that φ is an isomorphism, thereby proving the result. (Note: There are two parts to this. You must show that φ is bijctive, and that it is a homomorphism.)

   Proof. We first show that φ is bijective. Indeed, given a permutation $g : B \to B$, we obseve that $\theta^{-1} \circ g \circ \theta : A \to A$ is bijective as in part (a). Therefore $\psi : g \mapsto \theta^{-1} \circ g \circ \theta$ is a function from S_B to S_A. To see it is an inverse to φ we check that:

$$(\psi \circ \varphi)(f) = \psi(\theta \circ f \circ \theta^{-1}) = \theta^{-1} \circ (\theta \circ f \circ \theta^{-1}) \circ \theta = f,$$

   and similarly we can see that $(\varphi \circ \psi)(g) = g$. To conclude we must observe that φ is a homomorphism. Let $f, f' \in S_A$. Then:

$$\varphi(f) \circ \varphi(f') = (\theta \circ f \circ \theta^{-1}) \circ (\theta \circ f' \circ \theta^{-1}) = \theta \circ (f \circ f') \circ \theta^{-1} = \varphi(f \circ f'),$$

   as desired. □

8. The set S_3 has 6 elements. Compute the order and cycle decomposition of each element.

Proof.
- The identity permutation (1) which has order 1.
- The permutation swapping 1 and 2 and fixing 3. This is (1 2) and has order 2.
- The permutation swapping 1 and 3 and fixing 2. This is (1 3) and has order 2.
- the permutation swapping 2 and 3 and fixing 1. This is (2 3) and has order 2.
- The permutation sending 1 to 2, 2 to 3, and 3 to 1. This is (1 2 3) and has order 3.
- The permutation sending 1 to 3, 3 to 2, and 2 to 1. This is (1 3 2) and has order 3.

□