Homework Assignment 3

Due Friday, February 14

In problems 1-4 we establish some important basic results about group homomorphisms. For all four problems we fix a homomorphism $\varphi : G \to H$.

1. (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. $\square$

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

Proof. Notice that

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

Applying for example problem 7 from homework 2 we see also that $\varphi(x)\varphi(x^{-1}) = 1_H$, so that by the uniqueness of the inverse of $\varphi(x)$ we are done. $\square$

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

Proof. We begin by proving something slightly more general.

Lemma 1. *Suppose h is the element of a group and $|h| = n$. If $h^d = 1$ for some $d \geq 0$ then $n|d$.*

Proof. If $d = 0$ then it is trivial for n to divide d, so we can assume that $d > 0$. Then by definition of order, we have $n < d$. We use division with remainder for d/n to see that $d = nq + r$ for remainder $0 \leq r < n$. Notice then that

$$1 = h^d = h^{nq+r} = (h^n)^q h^r = 1 \cdot h^r = h^r.$$

But as $r < n$ this implies $r = 0$. Therefore $d = nq$ and $n|d$. $\square$

This lemma makes the proof rather easy. Suppose $|g| = d$ and $|\varphi(g)| = n$. Then:

$$\varphi(g)^d = \varphi(g^d) = \varphi(1) = 1.$$

Thus applying the lemma we have $n|d$. $\square$

(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 a homomorphism. 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. $\square$

(e) Conclude 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 $n = m$. □

2. Define the *kernel* of φ to be

$$\ker \varphi = \{g \in G : \varphi(g) = 1_H\}$$

(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 φ is injective if and only if $\ker \varphi = \{1_G\}$.

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. More generally, for $h \in H$ define the *fiber over* h to be

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

(a) Show that $\ker \varphi = \varphi^{-1}(1)$

Proof. This is the definition of $\ker \varphi$. □

(b) 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. □

(c) 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. □

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

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. Define the *image* of φ to be

$$\operatorname{im}\varphi = \{h \in H : h = \varphi(g) \text{ for some } g \in G\}.$$

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. □

Recall that we defined the kernel of a group action in class. The following exercise shows that the kernel of a homomorphism and the kernel of a group action are related, justifying our terminology.

5. Let $G \times A \to A$ be an action of G on a set A. Let $\varphi : G \to \operatorname{Aut}(A)$ be the associated permutation representation. 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 $\varphi(g) = \sigma_g \in \mathrm{Aut}(A)$. 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 of the automorphism group of A. In particular, $\varphi(g) = 1_{\mathrm{Aut}(A)}$ 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. □

6. Describe an injective homomorphism from $\varphi : D_{2n} \to S_n$ (you may describe this in words). In the map you described, what is the cycle decomposition of $\varphi(r)$ (where as usual r is the generator corresponding to rotation of the n-gon by $2\pi/n$)?

Proof. We describe the homomorphism as follows. Label the vertices of the n-gon as $1, 2, 3, \cdots, n$. Then view an element of D_{2n} as a symmetry of the n-gon, and notice that it permutes the integers 1 through n by paying attention to where they land. In particular, each symmetry induces a permutation of the integers 1 through n, which is an ement of S_n. This identification of a symmetry with a permutation will be the homomorphism φ. Notice also that composing two symmetries will compose the two permutations, so that this identification is in fact a homomorphism. Now 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 $(1\ 2\ 3 \cdots n-1\ n)$. □

7. 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.

□