Math 31 – Homework 5 Solutions

Easier

1. Determine if each mapping is a homomorphism. State why or why not. If it is a homomorphism, find its kernel, and determine whether it is one-to-one and onto.

(a) Define $\varphi : \mathbb{Z} \to \mathbb{R}$ by $\varphi(n) = n$. (Both are groups under addition here.)

(b) Let G be a group, and define $\varphi : G \to G$ by $\varphi(a) = a^{-1}$ for all $a \in G$.

(c) Let G be an *abelian* group, and define $\varphi : G \to G$ by $\varphi(a) = a^{-1}$ for all $a \in G$.

(d) Let G be a group, and define $\varphi : G \to G$ by $\varphi(a) = a^2$ for all $a \in G$.

Solution. (a) Yes, this is a homomorphism. We clearly have

$$\varphi(n + m) = n + m = \varphi(n) + \varphi(m)$$

for all $n, m \in \mathbb{Z}$. Since $\varphi(n) = 0$ if and only if $n = 0$, we see that $\ker \varphi = \{0\}$. Since the kernel is trivial, φ is one-to-one. It is not onto, since the image consists only of the integers, which form a proper subset of $\mathbb{R}$.

(b) This is *not* a homomorphism. If $a, b \in G$, then $\varphi(ab) = (ab)^{-1} = b^{-1}a^{-1}$, which is not equal to $\varphi(a)\varphi(b) = a^{-1}b^{-1}$ in general.

(c) When G is abelian, this map is a homomorphism. From the computation we did in part (b), we see that

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

Note that if $a \in \ker \varphi$, then $e = \varphi(a) = a^{-1}$, which means that $a = e$, and $\ker \varphi = \{e\}$. This implies that φ is one-to-one. It is also onto: if $a \in G$, then

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

Thus φ is an isomorphism from G to G, or an automorphism of G.

(d) This is not a homomorphism in general. If $a, b \in G$, then $\varphi(ab) = (ab)^2 = abab$, which is not necessarily equal to a^2b^2. In fact, φ is a homomorphism if and only if G is abelian.

2. Consider the subgroup $H = \{i, m_1\}$ of the dihedral group D_3. Find all the left cosets of H, and then find all of the right cosets of H. Observe that the left and right cosets do not coincide.

Solution. The left cosets are

$$H = \{i, m_1\}$$
$$r_1H = \{r_1, m_3\}$$
$$r_2H = \{r_2, m_2\},$$

while the right cosets are

$$H = \{i, m_1\}$$
$$Hr_1 = \{r_1, m_2\}$$
$$Hr_2 = \{r_2, m_3\}.$$

These do not coincide. Note that in particular this shows that H is not normal in D_3.

3. Find the cycle decomposition and order of each of the following permutations.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 4 & 2 & 7 & 6 & 9 & 8 & 5 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 3 & 4 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 \end{pmatrix}$

Solution. (a) The cycle decomposition is

$$(1\ 3\ 4\ 2)(5\ 7\ 9).$$

Since the cycles have length 4 and 3, the order of this permutation is 12.

(b) The cycle decomposition is

$$(1\ 7)(2\ 6)(3\ 5),$$

and the order is clearly 2.

(c) We'll decompose both permutations into disjoint cycles, and then multiply them. The first is

$$(1\ 7)(2\ 6)(3\ 5\ 4),$$

and the second is

$$(1\ 2\ 3)(4\ 5\ 6\ 7).$$

Therefore, the product is

$$(1\ 7)(2\ 6)(3\ 5\ 4)(1\ 2\ 3)(4\ 5\ 6\ 7) = (1\ 6)(2\ 5)(3\ 7).$$

Again, the order is simply 2.

4. Determine whether each permutation is even or odd.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 5 & 1 & 3 & 7 & 8 & 9 & 6 \end{pmatrix}$

(b) $(1\ 2\ 3\ 4\ 5\ 6)(7\ 8\ 9)$

(c) $(1\ 2\ 3\ 4\ 5\ 6)(1\ 2\ 3\ 4\ 5\ 7)$

(d) $(1\ 2)(1\ 2\ 3)(4\ 5)(5\ 6\ 8)(1\ 7\ 9)$

Solution. (a) We'll first convert the permutation to cycle notation, and then write it as a product of transpositions:

$$(1\ 2\ 4)(3\ 5)(6\ 7\ 8\ 9) = (1\ 4)(1\ 2)(3\ 5)(6\ 9)(6\ 8)(6\ 7).$$

We can see that this permutation is even.

(b) In terms of transpositions, we have

$$(1\ 6)(1\ 5)(1\ 4)(1\ 3)(1\ 2)(7\ 9)(7\ 8),$$

so the permutation is odd.

(c) The first cycle is the same as in the previous part, so we just need to know the parity of the second:

$$(1\ 7)(1\ 5)(1\ 4)(1\ 3)(1\ 2).$$

This is odd, as is the first cycle, so the whole permutation is even.

(d) By now you've probably noticed that a 3-cycle can be written as a product of two transpositions, so it is even. We have three 3-cycles and two transpositions, so the permutation is even.

5. Let G and G' be groups, and suppose that $|G| = p$ for some prime number p. Show that any group homomorphism $\varphi : G \to G'$ must either be the trivial homomorphism or a one-to-one homomorphism.

Proof. Let $\varphi : G \to G'$ be a homomorphism. We know that $\ker \varphi$ is a subgroup of G, so its order must divide $|G|$ by Lagrange's theorem. Since $|G| = p$ is prime, we must have either $|\ker \varphi| = 1$ or $|\ker \varphi| = p$. In the first case, $\ker \varphi = \{e\}$, so φ is one-to-one. In the second case, $\ker \varphi = G$, so φ must be the trivial homomorphism.

Medium

6. [Saracino, #12.13 modified] Let $\varphi : G \to G'$ be a group homomorphism. If G is abelian and φ is onto, prove that G' is abelian.

Proof. We need to show that if $x, y \in G'$, then $xy = yx$. Since φ is onto, we can write $x = \varphi(a)$ and $y = \varphi(b)$ for some $a, b \in G$. We then have

$$xy = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba),$$

since G is abelian. But then,

$$xy = \varphi(ba) = \varphi(b)\varphi(a) = yx,$$

so x and y indeed commute. Since x and y were arbitrary, G' is an abelian group.

7. [Saracino, #12.3 and 12.20 modified] Let G be an abelian group, n a positive integer, and define $\varphi : G \to G$ by $\varphi(x) = x^n$.

(a) Show that φ is a homomorphism.

Proof. Let $a, b \in G$. Then since G is abelian, we have

$$\varphi(ab) = (ab)^n = a^n b^n = \varphi(a)\varphi(b),$$

so φ is a homomorphism.

(b) Suppose that G is a finite group and that n is relatively prime to $|G|$. Show that φ is an automorphism of G.

Proof. We saw in part (a) that φ is a homomorphism, so we simply need to prove that it is one-to-one and onto. To see that φ is one-to-one, suppose that $a \in \ker \varphi$, i.e., that $\varphi(a) = e$. Then $a^n = e$, so $o(a)$ must divide n. But $o(a)$ also divides $|G|$ by Lagrange's theorem, and since $\gcd(n, |G|) = 1$, we must have $o(a) = 1$. Therefore, $a = e$, so $\ker \varphi = \{e\}$, and φ is one-to-one. Since G is a finite group, any one-to-one map from G to G is necessarily onto. Therefore, φ is an automorphism of G.

8. [Saracino, #12.33 modified] Let $V_4 = \{e, a, b, c\}$ denote the Klein 4-group. Since $|V_4| = 4$, Cayley's theorem tells us that V_4 is isomorphic to a subgroup of S_4. In this problem you will apply techniques from the proof of the theorem to this specific example in order to determine which subgroup of S_4 is matched up to V_4.

Suppose we label the elements of the Klein 4-group using the numbers 1 through 4, in the following manner:

$$\begin{matrix} e & a & b & c \\ 1 & 2 & 3 & 4 \end{matrix}$$

Now multiply every element by a in order, i.e.,

$$\begin{matrix} e & a & b & c \\ 1 & 2 & 3 & 4 \end{matrix} \quad \longrightarrow \quad \begin{matrix} a & e & c & b \\ 2 & 1 & 4 & 3 \end{matrix}$$

Then multiplication by a determines a permutation of V_4 (by the proof of Cayley's theorem). This corresponds to an element of S_4 via the labels that we have given the elements of V_4. Do this for every element x of V_4. That is, write down the permutation in S_4 (in cycle notation) that is obtained by multiplying every element of V_4 by x.

Proof. Certainly multiplication by the identity e yields the identity permutation ι. Also, we have shown above that a corresponds to the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$

which is

$$(1\ 2)(3\ 4)$$

in cycle notation. Similarly, if we multiply every element by b, we have

$$\begin{matrix} e & a & b & c \\ 1 & 2 & 3 & 4 \end{matrix} \quad \longrightarrow \quad \begin{matrix} b & c & e & a \\ 3 & 4 & 1 & 2 \end{matrix}$$

which results in the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix},$$

or

$$(1\ 3)(2\ 4)$$

in cycle notation. Finally, c yields

$$\begin{matrix} e & a & b & c \\ 1 & 2 & 3 & 4 \end{matrix} \quad \longrightarrow \quad \begin{matrix} c & b & a & e \\ 4 & 3 & 2 & 1 \end{matrix}$$

which gives the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

or

$$(1\ 4)(2\ 3).$$

Therefore, the subgroup of S_4 which is isomorphic to V_4 is

$$\{\iota, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

Hard

9. [Saracino, #10.32 modified] Let G be a group with identity element e, and let X be a set. A **(left) action of** G **on** X is a function $G \times X \to X$, usually denoted by

$$(g, x) \mapsto g \cdot x$$

for $g \in G$ and $x \in X$, satisfying:

1. $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$ for all $g_1, g_2 \in G$ and all $x \in X$.
2. $e \cdot x = x$ for all $x \in X$.

Intuitively, a group action assigns a permutation of X to each group element. (You will explore this idea in part (d) below.)

Finally, there are two important objects that are affiliated to any group action. For any $x \in X$, the **orbit of** x **under** G is the subset

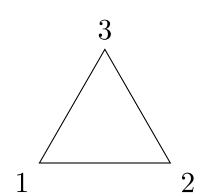
$$\text{orb}(x) = \{g \cdot x : g \in G\}$$

of X, and the **stabilizer of** x is the subset

$$G_x = \{g \in G : g \cdot x = x\}$$

of G.

(a) (Warm up.) We have already seen that it is possible to view the elements of the dihedral group D_3 as permutations of the vertices of a triangle, labeled as below:



Thus D_3 acts on the set $X = \{1, 2, 3\}$ of vertices by permuting them. Determine the orbit and stabilizer of each vertex under this action.

Solution. Let's start with the vertex 1. First note that if r_1 denotes counterclockwise rotation by 120 degrees,

$$r_1 \cdot 1 = 2,$$

so $2 \in \text{orb}(1)$. Also, $r_2 \cdot 1 = 3$, so $3 \in \text{orb}(1)$, and

$$\text{orb}(1) = \{1, 2, 3\} = X.$$

Similarly, you can check that

$$\text{orb}(2) = \text{orb}(3) = X$$

as well.

(b) (Another example.) Let G be a group, let $X = G$, and define a map $G \times X \to G$ by

$$(g, x) \mapsto g \cdot x = gx$$

for all $g \in G$ and $x \in X$, i.e., the product of g and x as elements of G. Verify that this defines a group action of G on itself. (This action is called **left translation**.) Given $x \in X = G$, what are $\text{orb}(x)$ and G_x?

Proof. To see that this is a group action, we need to check that if $g_1, g_2 \in G$ and $x \in X = G$, then $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$, and that $e \cdot x = x$. For the first one, observe that

$$g_1 \cdot (g_2 \cdot x) = g_1 \cdot (g_2 x) = g_1(g_2 x) = (g_1 g_2)x,$$

since multiplication in G is associative. For the second, note that

$$e \cdot x = ex = x$$

for all $x \in X$. Therefore, this defines an action of G on itself.

Now let $x \in X = G$. Then given any other $y \in X$, there exists $g \in G$ such that $g \cdot x = y$. In particular, $g = yx^{-1}$ works:

$$g \cdot x = gx = (yx^{-1})x = y.$$

Therefore, every element of X belongs to $\text{orb}(x)$, so

$$\text{orb}(x) = X$$

for all $x \in X$. (This says that the action is **transitive**.) Finally, note that if $x \in X$, then $g \cdot x = x$ if and only if $g = e$, so

$$G_x = \{e\}$$

for all $x \in X$. (A fancy way of wording this is to say that the action is **free**.)

(c) Prove that for every $x \in X$, the stabilizer G_x is a subgroup of G.

Proof. Let $x \in X$. Clearly $e \in G_x$, since $e \cdot x = x$ by definition. Now suppose that $g_1, g_2 \in G_x$. Then

$$(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = g_1 \cdot x = x,$$

since g_1 and g_2 both belong to the stabilizer of x. Therefore, $g_1 g_1 \in G_x$ as well, so G_x is closed. Finally, if $g \in G_x$, then $g \cdot x = x$, so

$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1} g) \cdot x = e \cdot x = x.$$

Thus $g^{-1} \in G_x$, and G_x is a subgroup of G.

(d) Given a fixed $g \in G$, define a function $\sigma_g : X \to X$ by

$$\sigma_g(x) = g \cdot x.$$

Show that σ_g is bijective, so σ_g defines a permutation of X. [Compare this to the proof of Cayley's theorem.]

Proof. To see that σ_g is one-to-one, suppose that $x, y \in X$ with $\sigma_g(x) = \sigma_g(y)$. Then

$$g \cdot x = g \cdot y,$$

so

$$g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g \cdot y).$$

But $g^{-1} \cdot (g \cdot x) = (g^{-1} g) \cdot x = x$, and similarly for y, so $x = y$ and σ_g is one-to-one. Now suppose that $y \in X$, and let $x = g^{-1} \cdot y$. Then

$$\sigma_g(x) = g \cdot x = g \cdot (g^{-1} \cdot y) = (g g^{-1}) \cdot y = y,$$

so σ_g is onto. Thus σ_g is a bijection.

(e) Recall that S_X denotes the group of permutations of X under composition. Define a function $\varphi : G \to S_X$ by

$$\varphi(g) = \sigma_g$$

for all $g \in G$. Prove that φ is a homomorphism. [Note: The proof of Cayley's theorem is a special case of this phenomenon, with G acting on itself by left translation.]

Proof. We simply need to check that $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ for all $g_1, g_2 \in G$, i.e. that

$$\sigma_{g_1 g_2} = \sigma_{g_1} \circ \sigma_{g_2}.$$

If $x \in X$, then

$$\sigma_{g_1 g_2}(x) = (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = \sigma_{g_1}(\sigma_{g_2}(x)) = \sigma_{g_1} \circ \sigma_{g_2}(x).$$

Since x was arbitrary, we have $\sigma_{g_1 g_2} = \sigma_{g_1} \circ \sigma_{g_2}$. Therefore, φ is a homomorphism.

Parts (d) and (e) above show that a group action gives an alternative way of viewing a group as a collection of symmetries (or permutations) of some object. Cayley's theorem provides a specific example, where a group is viewed as a collection of permutations of itself. Group actions provide one of the most interesting ways in which groups are used in practice.