Math 412. Homomorphisms of Groups: Answers

DEFINITION: A **group homomorphism** is a map $G \xrightarrow{\phi} H$ between groups that satisfies $\phi(g_1 \circ g_2) = \phi(g_1) \circ \phi(g_2)$.

DEFINITION: An **isomorphism** of groups is a bijective homomorphism.

DEFINITION: The **kernel** of a group homomorphism $G \xrightarrow{\phi} H$ is the subset

$$\ker \phi := \{g \in G \mid \phi(g) = e_H\}.$$

THEOREM: A group homomorphism $G \xrightarrow{\phi} H$ is injective if and only if $\ker \phi = \{e_G\}$, the trivial group.

THEOREM: A non-empty subset H of a group $(G, \circ)$ is a **subgroup** if and only if it is closed under $\circ$, and for every $g \in H$, the inverse g^{-1} is in H.

A. EXAMPLES OF GROUP HOMOMORPHISMS

(1) Prove that (one line!) $GL_n(\mathbb{R}) \to \mathbb{R}^\times$ sending $A \mapsto \det A$ is a group homomorphism.[1] Find its kernel.
(2) Show that the canonical map $\mathbb{Z} \to \mathbb{Z}_n$ sending $x \mapsto [x]_n$ is a group homomorphism. Find its kernel.
(3) Prove that $\nu : \mathbb{R}^\times \to \mathbb{R}_{>0}$ sending $x \mapsto |x|$ is a group homomorphism. Find its kernel.
(4) Prove that $\exp : (\mathbb{R}, +) \to \mathbb{R}^\times$ sending $x \mapsto 10^x$ is a group homomorphism. Find its kernel.
(5) Consider 2-element group $\{\pm\}$ where $+$ is the identity. Show that the map $\mathbb{R}^\times \to \{\pm\}$ sending x to its sign is a homomorphism. Compute the kernel.
(6) Let $\sigma : D_4 \to \{\pm 1\}$ be the map which sends a symmetry the square to 1 if the symmetry preserves the orientation of the square and to -1 if the symmetry reserves the orientation of the square. Prove that σ is a group homomorphism with kernel R_4 of rotations of the square.

(1) $\det(AB) = \det A \det B$ from Math 217, so the determinant map is a group homomorphism. The kernel is $SL_n(\mathbb{R}) := \{A \in GL_n(\mathbb{R}) \mid \det A = 1\}$.
(2) We know $[x + y]_n = [x]_n + [y]_n$, so $x \mapsto [x]_n$ is a group homomorphism. The kernel is $n\mathbb{Z} := \{nk \,|\, k \in \mathbb{Z}\}$.
(3) $\nu(xy) = \nu(x)\nu(y)$ because $|xy| = |x||y|$ for all real numbers. The kernel is $\{\pm 1\}$.
(4) $\exp(x + y) = 10^{x+y} = 10^x 10^y = \exp(x) \exp(y)$ so exp is a group homomorphism. Its kernel is $\{0\}$.
(5) Call the map f. So $f(x) = +$ if x is positive and $f(x) = -$ if x is negative. We know $f(xy) = +$ if x, y are both positive, and $f(xy) = -$ if one of them is positive and the other negative. Thus $f(xy) = f(x)f(y)$ according to the group operation we put on the set $\{\pm\}$. Since the identity element of the group $\{\pm\}$ is $+$, the kernel is $\mathbb{R}_{>0}$, the set of all positive real numbers.
(6) Rotations preserve orientation, and reflections change it. That is, $\phi(\{e, r_1, r_2, r_3\}) = 1$ and $\phi(\{x, y, d, a\}) = -1$. Since the product of two rotations is a rotation, the product of two reflections is a rotation, and the product of a rotation and a reflection is a reflection, this says the map is a homomorphism. The kernel is the rotation subgroup $R_4 = \{e, r_1.r_2, r_3\}$.

B. KERNEL AND IMAGE.

Let $G \xrightarrow{\phi} H$ be a group homomorphism.

(1) Prove that the image of ϕ is a subgroup of H.
(2) Prove that the kernel of ϕ is a subgroup of G.

[1] In this problem, and often, you are supposed to be able to infer what the operation is on each group. Here: the operation for both is multiplication, as these are both groups of units in familiar rings.

(3) Prove that ϕ is injective if and only if $\ker \phi = \{e_G\}$.
(4) For each homomorphism in A, decide whether or not it is injective. Decide also whether or not the map is an isomorphism.

These are the kind of straightforward proofs you MUST practice doing to do well on quizzes and exams.

(1) $\phi(e) = \phi(e \circ e) = \phi(e)\phi(e)$. Now composing both sides on the left with $\phi(e)^{-1}$, we have $e = \phi(e)$.
(2) We have $g \circ g^{-1} = e$. So applying ϕ, $\phi(g \circ g^{-1}) = \phi(g) \circ \phi(g^{-1}) = e$. Because we can also do this in the other order, we see that $\phi(g^{-1})$ is the inverse of $\phi(g)$, as needed.
(3) See the proof in the book, Theorem 7.20 (3), page 221.
(4) You have done "the same proof" at least in three different settings, starting in 217, next with rings in Chapter 3. Here is the proof for good measure: Let $K \subset G$ be the kernel. To show it is a subgroup of G, we must show
   (a) K is non-empty
   (b) If $g_1, g_2 \in K$, then $g_1 g_2 \in K$.
   (c) If $g \in K$, then g^{-1} in K.
   We check each: for (a), note that $\phi(e_G) = e_H$ so $e_G \in K$ and K is not empty. For (b), note that $\phi(g_1 g_2) = \phi(g_1)\phi(g_2) = e_H e_H = e_H$, so $g_1 g_2 \in K$. For (c), note that $gg^{-1} = e_G$, so $\phi(g)\phi(g^{-1}) = \phi(e_G) = e_H$. But since $g \in K$, this says $\phi(g)\phi(g^{-1}) = e_H \phi(g^{-1}) = \phi(g^{-1}) = e_H$, so also $g^{-1} \in K$. QED.
(5) Again, this is the kind of straightforward problem you MUST practice doing to do well on quizzes and exams. Not only that, but you have done "the same proof" at least in three different settings, starting in 217, next with rings in Chapter 3. It is in the book as Theorem 8.17 on page 264. Please come see me if you are not sure you are doing correctly.
(6) The only injective homomorphism in A is (4). But it is not surjective, as the image consists only of the positive real numbers. So none of the maps in A is an isomorphism.

C. Classification of Groups of order 2 and 3

(1) Prove that any two groups of order 2 are isomorphic.
(2) Give three natural examples of groups of order 2: one additive, one multiplicative, one using composition. [Hint: Groups of units in rings are a rich source of multiplicative groups, as are various matrix groups. Dihedral groups such as D_4 and its subgroups are a good source of groups whose operation is composition.]
(3) Suppose that G is a group with three elements $\{e, a, b\}$. Construct the group operation table for G, explaining the Sudoku property of the group table, and why it holds.
(4) Explain why any two groups of order three are isomorphic.
(5) Give two natural examples of groups of order 3, one additive, one using composition. Describe the isomorphism between them.

(1) Let G and H be groups of order 2. Say $G = \{e_G, g\}$ and $H = \{e_H, h\}$. We can write out the table for G and H. Note that we know the first row and column, by definition of identity. So the only mystery is what is $g \star g$ in G and what is $h \star h$ in H. But since $g \in G$ must have an inverse, we must have $g^2 = e_G$, otherwise g would have no inverse. Likewise, we must have that $h^2 = e_H$. So the tables look the same: the first row is $e \;\; g \; (or \; h)$ and the second row is $g \, (or \; h) h \;\; e$. This means that the bijection $e_G \mapsto e_H$ and $g \mapsto h$ is a group homomorphism.
Examples: $(\mathbb{Z}_2, +), (\mathbb{Z}^\times, \times) = (\{\pm 1\}, \times)$ and the group of bijections between two objects are all examples.
(2) The Sudoku property says that no row (or column) of the table can have the same element appearing more than once. Indeed, suppose some row of a group table has the same entry twice. If the row is telling us $a \star --$, then there must be two columns, indexed by say b and c, such that $a \star b = a \star c$. But now multiply both side by a^{-1} to see that $b = c$. This contradiction tells us that the row can not have any element appearing more than once. A similar argument works for columns.
(3) Make the table:

♡	e	a	b
e	e	a	b
a	a		
b	b		

We see that we can not have $a^2 = a$ because that would force $a = e$. Likewise, if $a^2 = e$, then the Sudoku property would force $ab = b$, which again forces $a = e$. So it must be that $a^2 = b$. Now the Sudoku property force that $ab = e$. Finally there is only one way to fill in the next and final row. So the table must be

♡	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

(4) So any group of three elements, after renaming, is isomorphic to this one.
(5) $(\mathbb{Z}_3, +)$ is an additive group of order three. The group R_3 of rotational symmetries of an equilateral triangle is another group of order 3. Its elements are the rotation through 120^0, the rotation through 240^0, and the identity. An isomorphism between them sends $[1]$ to the rotation through 120. This forces $[2] \mapsto$ rotation through 240, and $[0] \mapsto e$.

D. CLASSIFICATION OF GROUPS OF ORDER 4: Suppose we have a group G with four elements a, b, c, e.

(1) Prove that we can't have both ab and ac equal to e. So swapping the names of b and c if necessary, we can assume that $ab \neq e$.
(2) Prove that given any group G of four elements, after changing names if necessary, we can assume that the elements are e, a, b, c where $ab = c$.
(3) Given a group with 4 elements, without loss of generality as in (2), make a table for the group G, filling in only as much information as you know for sure.
(4) There are three possible ways to complete the tables you started in (3). Make three separate tables for these three ways.
(5) Show that two of the three groups you found in (4) are isomorphic to each other, but that the third is not isomorphic to any other.
(6) Explain why, up to isomorphism, there are exactly two groups of order 4. We call these the **cyclic group of order 4** and the **Klein 4-group**, respectively. Which is which among your tables? What are good examples of each using additive notation? What are good examples among symmetries of the squares?

(1) If $ab = ac = e$, then multiplying by a^{-1} on the left, we see $b = c$.
(2) Assume $ab \neq e$. That means $ab = c$, since both $ab = a$ and $ab = b$ lead to contradictions: $ab = a$ gives $b = e$ and $ab = b$ given $a = e$, both impossible.
(3) Make the table:

♠	e	a	b	c
e	e	a	b	c
a	a		c	
b	b			
c	c			

(4) So either $a^2 = e$ or $a^2 = b$. Both give valid groups whose tables can be filled out using the Sudoku property.

If $a^2 = b$, we get

♡	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

. If $a^2 = e$, we have either

♣	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

or

♢	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

.

(5) Note that in table ♢, every element is self-inverse, but that is not true in the other two groups. So ♢ is not isomorphic to either of the other two. The remaining two are isomorphic: we know e must correspond to e, and that b in ♡ must map to a in ♣ because these are the only elements of order two in their respective groups. The map $e \mapsto e$, $a \mapsto b$, $b \mapsto a$ and $c \mapsto c$ is an isomorphism.
(6) So any group of four elements, after renaming, is isomorphic to either ♣ or ♢ above. The first is the cyclic group of order 4, which has two elements of order 4, and one of order 2. The second is the Klein four group, which has 3 elements of order 2, represented by ♢ above.
(7) Good representatives are $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ and $(\mathbb{Z}_4, +)$. We can also find nice representatives in D_4. The group R_4 of rotational symmetries of a square is a cyclic group of order 4, so isomorphic to $\mathbb{Z}_4$. The subgroup generated by the vertical and horizonal reflections is an example of a Klein 4-group, so isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

E. CYCLIC GROUPS.

(1) Show that any two cyclic groups of the same order are isomorphic.
(2) Prove that a cyclic group is always abelian.
(3) Use Lagrange's Theorem to show that if G has prime order, then G is cyclic. Even better, show that for every $g \in G$, $g \neq e$, we have $G = \langle g \rangle$.

(1) Suppose G and H are generated by g, h respectively, and both have order n. Then $G = \{e_G, g, g^2, \ldots, g^{n-1}\}$ and $H = \{e_H, h, h^2, \ldots, h^{n-1}\}$. The map that send $g^i \mapsto h^i$ clearly respects the group structure, since $g^i \circ g^j = g^{i+j}$.
(2) Easy: $g^i \circ g^j = g^j \circ g^i = g^{i+j}$.
(3) Say $|G| = p$, prime. Take any non-identity $g \in G$. Since $|g||G| = p$, it must be that $|g| = p$. But then $\langle g \rangle$ has p elements, and must be G.

F. GROUPS OF SMALL ORDER.

(1) Up to isomorphism, there are exactly six groups of order at most five. Explain.
(2) List one representative of each of the six isomorphism types from (1).
(3) What is the smallest possible order of a non-abelian group? Give an example.

G. Let $\phi : G \to H$ be a group homomorphism.

(1) For any $g \in G$, prove that $|\phi(g)| \leq |g|$. [Here $|g|$ means the order of the element g.]
(2) For any $g \in G$, prove that $|\phi(g)|$ divides $|g|$. [Hint: Name the orders! Say $|\phi(g)| = d$ and $|g| = n$. Use the division algorithm to write $n = qd + r$, with $r < d$. What do you want to show about r?]
(3) Prove that the map $\mathbb{Z}_4 \to \mathbb{Z}_4$ which fixes $[0]$ and $[2]$ but swaps $[1]$ and $[3]$ is an isomorphism. An isomorphism of a group to itself is also called an **automorphism.**

(1) Say g has order n. So $g^n = e_G$. This means $\phi(g^n) = (\phi(g))^n = e_H$. So $\phi(g)$ has order at most n.
(2) Say $\phi(g)$ has order d. Then write $n = dq + r$ for some remainder $0 \leq r \leq d-1$. So $e_H = (\phi(g))^n = (\phi(g))^{qd+r} = ((\phi(g))^d)^q(\phi(g))^r = (\phi(g))^r$. But this says that $\phi(g)$ has order at most $r < d$, a contradiction unless $r = 0$. So $d|n$.
(3) Call the map f. We need to check that $f([a]_4 + [b]_4) = f([a]_4) + f([b]_4)$ for all $[a]_4, [b]_4$. There are 16 different pairs of values for $[a]$ and $[b]$ to check, but since the group $\mathbb{Z}_4$ is abelian, we need only check 8 of these. Also, if the $[a]$ and $[b]$ are both either $[0]$ or $[2]$, it is true since f does nothing to $[0]$ or $[2]$. The five remaining things to check are that $f([1] + [3]) = f([1]) + f[3])$ which is true since both are zero, $f([0] + [3]) = f([0]) + f[3])$ which is true since both are $[1]$, $f([0] + [1]) = f([0]) + f[1])$ which is true since both are $[3]$, $f([2] + [1]) = f([2]) + f[1])$ which is true since both are $[1]$, and $f([2] + [3]) = f([2]) + f[3])$ which is true since both are $[3]$.

H. Let $\phi : R \to S$ be a ring homomorphism.

(1) Show that $\phi : (R, +) \to (S, +)$ is a group homomorphism.
(2) Show that $\phi : (R^\times, \times) \to (S^\times, \times)$ is a group homomorphism.
(3) Explain how the two different kernels in (1) and (2) give two subsets of R that are groups under two different operations.
(4) Consider the canonical ring homomorphism $\mathbb{Z} \to \mathbb{Z}_{24}$ sending $x \mapsto [x]_{24}$. Describe these two kernels explicitly. Prove that one is isomorphic to $\mathbb{Z}$ and one is the trivial group.

(1) This is immediate from the definition of ring homomorphism, as $\phi(x + y) = \phi(x) + \phi(y)$ is one of the axioms.
(2) This also from the defintion of ring homomorphism, as $\phi(xy) = \phi(x)\phi(y)$ is one of the axioms. We do need to check that the target is in the right place, though. That is, we need to know that a unit goes to a unit under a ring homomorphism. We proved this before.
(3) The kernels of the two maps in (1) and (2) are both subsets of R. But they have a different binary operation on them, namely $+$ and $\times$.
(4) The kernel of the canonical map is the additive $24\mathbb{Z}$. The map $\mathbb{Z} \to 24\mathbb{Z}$ sending $n \mapsto 24n$ is easily checked to be a bijective homomorphism, so isomorphism. The map of units is $\mathbb{Z}^\times = \{\pm 1\} \to \mathbb{Z}_{24}^\times$. Since $1 \neq -1$ in $\mathbb{Z}_{24}$, the map is injective, and the kernel is the trivial group $\{1\}$.