Math 412. Adventure Sheet on Homomorphisms of Groups.

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

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

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 the 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 that sends a symmetry of 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, the rotations of the square.

Solution.

(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 $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$.
(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 $\phi(e_G) = e_H$.
(2) Prove that the image of ϕ is a subgroup of H.

[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) Make a table for the group G, filling in only as much information as you know for sure.
(4) There are two possible ways to fill in $a^2 = a \circ a$ in your table. Draw two tables, and complete as much of each table as you can. One table can be completely determined, the other can not.
(5) There should be two possible ways to complete the remaining table. Show that these give isomorphic groups.
(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?

E. Let $\phi : G \to H$ be a group homomorphism.
(1) For any $g \in G$, prove that $|\phi(g)| \leqslant |g|$. [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 $\mathbb{Z}_4 \to \mathbb{Z}_4$ that fixes $[0]$ and $[2]$ but swaps $[1]$ and $[3]$ is an isomorphism. An isomorphism of a group to itself is also called an **automorphism.**

F. 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.
(5) Show that if m, n are coprime, then $\mathbb{Z}_{nm}^\times \cong \mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$.

THEOREM: If $\mathbb{F}$ is a finite field, then $\mathbb{F}^\times$ is a cyclic group.

G. Verify the theorem above by finding a generator for each of the groups: $\mathbb{Z}_5^\times, \mathbb{Z}_7^\times, (\mathbb{Z}_2[x]/(x^2 + x + 1))^\times$.

H. Proof of the theorem.
(1) Show that, if $|g|$ is finite and $n \in \mathbb{N}$, then $|g^n| \mid |g|$.
(2) Show that, if $|g| = nd$, then $|g^n| = d$.
(3) Let G be a finite abelian group, and $a, b \in G$. Show that if $(|a|, |b|) = 1$, then $|ab| = |a||b|$.
(4) Let G be a finite abelian group. Let $c \in G$ be such that $|a| \leqslant |c|$ for all $a \in G$. Show that $|a| \mid |c|$ for all $a \in G$.[2]
(5) Let $\mathbb{F}$ be a finite field, and $a, c \in \mathbb{F}^\times$. Show that if $|a| \mid |c|$, then a is a root of the polynomial $f(x) = x^{|c|} - 1 \in \mathbb{F}[x]$.
(6) Conclude the proof of the theorem.

[2]Hint: Suppose that there is some $a \in G$ with $|a| < |c|$, but $|a| \nmid |c|$. Use the previous parts to find an element with order larger than $|c|$.

(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:

$\heartsuit$	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

$\heartsuit$	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 cannot 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) Assuming (without loss of generality) that $ab \neq e$, show that $ab = c$.

(3) Make a table for the group G, filling in only as much information as you know for sure.

(4) There are two possible ways to fill in $a^2 = a \circ a$ in your table. Draw two tables, and complete as much of each table as you can. One table can be completely determined, the other can not.

(5) There should be two possible ways to complete the remaining table. Show that these give isomorphic groups.

(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?

Solution.

(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:

$\spadesuit$	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

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

(5) Finally, 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

.

♣ is isomorphic to ♡: switch the a and b elements.

(6) So any group of four elements, after renaming, is isomorphic to one or the other of these. The first is the cyclic group of order 4, which has two elements of order 4, and one of order 2. (The identity is order 1 in any group). This is represented by table ♡. The second is the Klein four group, which has 3 elements of order 2.

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

(1) For any $g \in G$, prove that $|\phi(g)| \leqslant |g|$. [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 $\mathbb{Z}_4 \to \mathbb{Z}_4$ that fixes $[0]$ and $[2]$ but swaps $[1]$ and $[3]$ is an isomorphism. An isomorphism of a group to itself is also called an **automorphism.**

Solution.

(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 $0 \leqslant r \leqslant d - 1$. 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 $[3]$.

F. 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.
(5) Show that if m, n are coprime, then $\mathbb{Z}_{nm}^\times \cong \mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$.

Solution.

(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 $\{1\}$.
(5) This follows from the ring isomorphism $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

THEOREM: If $\mathbb{F}$ is a finite field, then $\mathbb{F}^\times$ is a cyclic group.

G. Verify the theorem above by finding a generator for each of the groups: $\mathbb{Z}_5^\times, \mathbb{Z}_7^\times, (\mathbb{Z}_2[x]/(x^2+x+1))^\times$.

Solution. $\mathbb{Z}_5^\times = \langle 2 \rangle$, $\mathbb{Z}_7^\times = \langle 3 \rangle$, $(\mathbb{Z}_2[x]/(x^2+x+1))^\times = \langle x \rangle$.

H. Proof of the theorem.

(1) Show that, if $|g|$ is finite and $n \in \mathbb{N}$, then $|g^n| \mid |g|$.
(2) Show that, if $|g| = nd$, then $|g^n| = d$.
(3) Let G be a finite abelian group, and $a, b \in G$. Show that if $(|a|, |b|) = 1$, then $|ab| = |a||b|$.
(4) Let G be a finite abelian group. Let $c \in G$ be such that $|a| \leqslant |c|$ for all $a \in G$. Show that $|a| \mid |c|$ for all $a \in G$.[2]
(5) Let $\mathbb{F}$ be a finite field, and $a, c \in \mathbb{F}^\times$. Show that if $|a| \mid |c|$, then a is a root of the polynomial $f(x) = x^{|c|} - 1 \in \mathbb{F}[x]$.
(6) Conclude the proof of the theorem.

Solution.

(1) Theorem 7.9 (a) in the book
(2) Theorem 7.9 (c) in the book
(3) For the inequality $|ab| \leqslant |a||b|$, we show that $(ab)^{|a||b|} = e$. Using the abelian axiom, $(ab)^{|a||b|} = a^{|a||b|}b^{|a||b|} = (a^{|a|})^{|b|}(b^{|b|})^{|a|} = e$. For the other inequality, suppose that $(ab)^k = e$. Then $a^k b^k = e$, so $a^k = b^{-k}$. Thus, $a^{k|b|} = (a^k)^{|b|} = (b^{-k})^{|b|} = (b^{|b|})^k = e$. We then

[2]Hint: Suppose that there is some $a \in G$ with $|a| < |c|$, but $|a| \nmid |c|$. Use the previous parts to find an element with order larger than $|c|$.

have $|a||k|b|$ by part (1), and since $(|a|, |b|) = 1$, $|a||k$. Likewise, $|b||k$, and again using coprimeness, $|a||b||k$. It follows that $|a||b| \leqslant |ab|$, and equality must hold.

(4) Suppose that there is some $a \in G$ with $|a| < |c|$, but $|a| \nmid |c|$. Write $|a| = p^r m$, and $|c| = p^s n$, with $(p, m) = (p, n) = 1$ and $r > s$ for some prime p. By part (2), $|a^m| = p^r$ and $|c^{p^s}| = n$. Then, by part (3), $|a^m c^{p^s}| = p^r n$. But, $p^r n > |c|$, which is a contradiction. Therefore, there is no such a.

(5) The assumption implies that $a^{|c|} = 1$.

(6) Let $t = \max\{|g| \mid g \in \mathbb{F}^\times\} \leqslant |\mathbb{F}^\times|$. By part (4), $|a| \mid t$ for all $a \in \mathbb{F}^\times$. By part (5), this means that every element of $\mathbb{F}^\times$ is a root of $f(x) = x^t - 1$. This is a polynomial in a polynomial ring over a field; since it has degree t, it has at most t roots, so $|\mathbb{F}^\times| \leqslant t$. Any element has order at most t, so we see that equality holds. Thus, there is an element of order $|\mathbb{F}^\times|$, so the group is cyclic.