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.

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

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 $ab = c$.

[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 $|\phi(g)| \leq |g|$. [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 $\mathbb{Z}_4 \to \mathbb{Z}_4$ 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 $|a| \leq |c|$ 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 $|c|$.