Math 412. Simple groups and the First Isomorphism Theorem

FIRST ISOMORPHISM THEOREM FOR GROUPS: Let $G \xrightarrow{\phi} H$ be a *surjective* group homomorphism with kernel K. Then $G/K \cong H$. More precisely, the map

$$G/K \xrightarrow{\overline{\phi}} H \qquad gK \mapsto \phi(g)$$

is a well-defined group isomorphism.

A group G is called **simple** if the only normal subgroups of G are $\{e\}$ and G itself.

A. Use the first isomorphism theorem to prove the following:

(1) For any field $\mathbb{F}$, the group $SL_n(\mathbb{F})$ is normal in $GL_n(\mathbb{F})$ and the quotient $GL_n(\mathbb{F})/SL_n(\mathbb{F})$ is isomorphic to $\mathbb{F}^\times$.
(2) For any n, the group A_n is normal in $\mathcal{S}_n$ and the quotient $\mathcal{S}_n/A_n$ is cyclic of order two.

Solution.

(1) Easy peasy: The determinant map $GL_2(\mathbb{F}) \to \mathbb{F}^\times$ is a surjective group homomorphism. Its kernel is $SL_2(\mathbb{F})$. So by the first isomorphism theorem, the quotient $GL_2(\mathbb{F})/SL_2(\mathbb{F}) \cong F^\times$.
(2) The sign map $S_n \to \{\pm 1\}$ is a homomorphism with kernel A_n. So the quotient $S_n/A_n \cong \{\pm 1\}$, which is a cyclic group of order two.

B. Let H be the subgroup of $\mathbb{Z} \times \mathbb{Z}$ generated by $(5, 5)$.

(1) Find an element of finite order and an element of infinite order in the quotient $\mathbb{Z} \times \mathbb{Z}/H$.
(2) Prove that
$$\psi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}_5 \quad (m, n) \mapsto (m - n, [n]_5)$$
is a group homomorphism.
(3) Prove that ψ is surjective and compute its kernel.
(4) Show that $(\mathbb{Z} \times \mathbb{Z})/H$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}_5$.

Solution.

(1) The coset $(1, 1) + H$ has order five, so finite. The coset $(1, 0) + H$ has infinite order, since $(n, 0) \notin H$ for any n.
(2) We check $\psi((a, b) + (m, n)) = \psi(a + m, b + n) = (a + m - (b + n), [b + n]_5) = ((a - b) + (m - n), [b]_5 + [n]_5) = ((a - b), [b]_5) + ((m - n), [n]_5) = \psi(a, b) + \psi(m, n)$.
(3) Take any $(m, [a]_5)$ in the target. Then $\psi(m + a, a) = (m, [a]_5)$, so the map is surjective. The kernel is H. Say $(5n, 5n) \in H$. Then $\psi(5n, 5n) = (5n - 5n, [5n]_5) = (0, [0]_5)$, so $H \subset \ker \psi$. Conversely, say $\psi(m, n) = 0$. Then $(m - n, [n]_5) = (0, [0]_5)$, so $m = n$, and also n (hence both) is a multiple of 5. So $(m, n) = (5d, 5d) \in H$. QED.
(4) Immediate from the First Isomorphism Theorem!

(5) The sign map $S_n \to \{\pm 1\}$ is a homomorphism with kernel A_n. So $S_n/A_n \cong \{\pm 1\}$, which is a cyclic group of order two.

C. Consider the map $(\mathbb{C}^\times, \times) \to (\mathbb{R}_{>0}, \times)$ sending z to $|z|$. Show that this is a surjective group homomorphism with kernel the circle group S^1. Describe the quotient $\mathbb{C}^\times/S^1$.

Solution. We've checked before that $|zw| = |z||w|$, which shows the map is a group homomorphism. It is surjective, since for any $a \in \mathbb{R}_{>0}$, $|a + 0i| = a$. The kernel is $\{z \in \mathbb{C}^\times \mid |z| = 1\} = S^1$. The First Isomorphism theorem guarantees that $\mathbb{C}^\times/S^1 \cong \mathbb{R}_{>0}$.

D. THE FIRST ISOMORPHISM THEOREM.

(1) Prove the First Isomorphism Theorem for Groups.
(2) What does the theorem say about group homomorphisms that are not necessarily surjective?
(3) Prove that if $f\colon G \longrightarrow H$ is a group homomorphism, then $|f(G)|\big||G|$.

Solution.

(1) First, we show that the map is well-defined. If $gK = g'K$, then $g' \in gK$, so $g' = gk$ for some $k \in K$. We then have $\phi(g') = \phi(gk) = \phi(g)\phi(k) = \phi(g)e = \phi(g)$. This show that the map is well-defined. Next, we show that it is a homomorphism: let $gK, hK \in G/K$. Then $\bar{\phi}(gK\, hK) = \bar{\phi}(ghK) = \phi(gh)$, and $\bar{\phi}(gK)\bar{\phi}(hK) = \phi(g)\phi(h) = \phi(gh)$, so $\bar{\phi}(gK\, hK) = \bar{\phi}(gK)\bar{\phi}(hK)$. Next, we show it is injective: if $\bar{\phi}(gK) = e$, then $\phi(g) = e$, so $g \in K$, which means that $gK = K$, the identity of G/K. Finally, the map is surjective, since for any $h \in H$, there is some $g \in G$ with $\phi(g) = h$, and thus $\bar{\phi}(gK) = h$.
(2) Given any group homomorphism $f : G \longrightarrow H$, we can apply the First Isomorphism Theorem to say that $\mathrm{im}(f) \cong G/\ker(f)$.
(3) Combining the Fist Isomorphism Theorem with Lagrange's Theorem, we get the following:
$$|f(G)||\ker(f)| = |G|.$$
In particular, $|f(G)|$ divides $|G|$.

E. SIMPLE GROUP WARMUP. Consider the groups $\mathbb{Z}$, $\mathbb{Z}_{35}$, $GL_5(\mathbb{Q})$, S_{17}, D_{100}. Find nontrivial normal subgroups for each of them. Are these groups simple?

Solution. $\mathbb{Z}$: any subgroup is normal.
$\mathbb{Z}_{35}$: any subgroup is normal. The nontrivial proper ones are $\langle 5\rangle$, $\langle 7\rangle$.
$GL_5(\mathbb{Q})$: $SL_5(\mathbb{Q})$.
S_{17}: A_{17}.
D_{100}: the subgroup of all the rotations. This is a normal subgroup because it has index 2.

F. EASY PROOFS. Let G be an arbitrary group.

(1) Prove that if G is simple, then every nontrivial[1] homomorphism $G \to H$ is *injective*.
(2) Prove that if G is simple, then every surjective homomorphism $G \to H$ is an isomorphism.

[1]By nontrivial, we mean the map does not send every element to e.

(3) If $G = H \times K$, where neither H nor K is trivial, then G is *not* simple.

Solution.

(1) The kernel of the homomorphism is a normal subgroup, and thus either G or $\{e\}$. Since our homomorphism is nontrivial, the kernel cannot be G, which means the homomorphism is injective.

(2) We have shown it must be injective, and since it is also surjective, it must be an isomorphism.

If a finite group G is not simple, there exists some nontrivial proper normal subgroup K of G and K and G/K are both smaller than G. We can think of G as being "made from" the smaller groups K and G/K. From this point of view, the simple groups are the basic building blocks, since we can't write them as "made from" smaller groups in this way.

THEOREM: If G is a finite abelian group, then G is simple if and only if it is cyclic of prime order.

THEOREM: The alternating groups $\mathcal{A}_n$ for $n \geqslant 5$ are simple.

There is a classification of all finite simple groups. It consists of a few infinite families (like $\{\mathbb{Z}_p \mid p \text{ prime}\}$ and $\{\mathcal{A}_n \mid n \geqslant 5\}$ and a few additional *sporadic* simple groups which do not belong to any of the families. The UM Math department played a big role in this classification: one of the sporadic simple groups is named after former department chair Jack McLaughlin, and the final and largest sporadic simple group, the Monster group, was discovered by current faculty member Robert Griess.

G. Prove the first theorem above: If G is a finite abelian group, then G is simple if and only if it is cyclic of prime order.[2]

Solution. Every subgroup of an abelian group is normal. The equivalence is now a problem from the homework.

H. PRODUCTS AND QUOTIENT GROUPS: Let K and H be arbitrary groups and let $G = K \times H$.

(1) Find a natural homomorphism $G \to H$ whose kernel K' is $K \times e_H$. Prove that $K \cong K'$.
(2) Prove that K' is a normal subgroup of G, whose cosets are all of the form $K \times h$ for $h \in H$.
(3) Prove that G/K' is isomorphic to H.

Solution.

(1) Consider the projection onto the second component, meaning the map $\phi : G \longrightarrow H$ given by $\phi(k, h) = h$. Then $(k, h) \in K'$ if and only if $h = e_H$, or equivalently, $(k, h) \in K \times e_H$.
(2) Since K' is the kernel of of a group homomorphism, K' is normal. Now note that for each $h \in H$,
$$K \times h = \{(k, h) : k \in K\} = (K \times e_H)\,(e_G, h).$$
On the other hand, given any K-coset $K'(k, h)$, $(e_G, h) = (k^{-1}, e_H)(k, h) \in K'(k, h)$. So every coset is of the form $K \times h$ for some h. Finally, if $h, h' \in H$, then $K \times h = K \times h'$ if and only if $(e, h')(e, h^{-1}) \in K \times \{e\}$, or equivalently, $h'h^{-1} = e$.
(3) The map in (1) is surjective, so this follows by the First Isomorphism Theorem.

I. APPLICATIONS OF SIMPLICITY OF $\mathcal{A}_n$, $n \geqslant 5$:

(1) Let $n \geqslant 5$ and $m \leqslant n$ be odd. Show that $\mathcal{A}_n$ is generated by m-cycles.[3]
(2) Show that if $n \geqslant 5$ and $m < n$, then there is no nontrivial action of $\mathcal{A}_n$ on a set of m elements.

[2]Hint: Reuse something you showed on the homework!

[3]Hint: Show that the subgroup of $\mathcal{A}_n$ generated by m-cycles is normal.

(3) Show that if $n \geqslant 5$ and $2 < m < n$, then there is no action of $\mathcal{S}_n$ on a set of m elements that has only one orbit.
(4) Show that the previous statement is false if $n = 4$.

Solution.

(1) We know that if we conjugate an m-cycle by any element of $\mathcal{S}_n$, we get another m-cycle. In particular, if we conjugate an m-cycle by any element of $\mathcal{A}_n$, we get another m-cycle. Now, consider the subgroup H of $\mathcal{A}_n$ generated by m-cycles. The inverse of an m-cycle is an m-cycle, so using the explicit form for the subgroup generated by elements, H is just the set of products of m-cycles. If we conjugate any element of H we get another product of m-cycles, which is an element of H. Thus, H is normal. Since $H \neq \{e\}$, $H = \mathcal{A}_n$.
(2) An action of $\mathcal{A}_n$ on a set of m elements yields an adjoint homomorphism $\mathcal{A}_n \to \mathcal{S}_m$. Since $n!/2 > n!/n \geq m!$, this map cannot be injective, so it must be the map sending everything to the identity. This corresponds to the trivial action.
(3) Consider the adjoint homomorphism $\mathcal{S}_n \to \mathcal{S}_m$ as above. If we restrict to the subgroup $\mathcal{A}_n$, we get the map sending everything to the identity, so $\mathcal{A}_n$ is contained in the kernel. We can then reinterpret our action as an action of $\mathcal{S}_n/\mathcal{A}_n \cong \mathbb{Z}_2$ on a set of m elements. Thus, any orbit has at most two elements, so there can't be just one orbit.
(4) Let $\mathcal{S}_4$ act on the set of pairings of four elements $\{\{\{1,2\},\{3,4\}\},\{\{1,3\},\{2,4\}\},\{\{1,4\},\{2,3\}\}\}$.