Final Exam

MATH 3175–Group Theory

Solutions

Problem 1. Let $f\colon G \to H$ be a function between two groups, and let $K := \{(x, y) \in G \times H \mid f(x) = y\}$ be its graph.

Suppose f is a homomorphism. Let $x_1, x_2 \in G$. Then $f(x_1x_2) = f(x_1)f(x_2)$, since f is a homomomorphism. Hence, since both G and H are groups, and by the definition of the group structure in the direct product of two groups,

$$(x_1, f(x_1)) * (x_2^{-1}, f(x_2)^{-1}) = (x_1, f(x_1)) * (x_2^{-1}, f(x_2^{-1})) = \\ (x_1x_2^{-1}, f(x_1)f(x_2^{-1})) = (x_1x_2^{-1}, f(x_1x_2^{-1})),$$

and this belongs to K. Therefore, K is a subgroup of $G \times H$.

Conversely, suppose K is a subgroup of $G \times H$. Then, for all $x_1, x_2 \in G$ we have $(x_1, f(x_1)) * (x_2, f(x_2)) = (x_1x_2, f(x_1)f(x_2)) \in K$, and so $f(x_1x_2) = f(x_1)f(x_2)$. Hence, f is a homomorphism.

Problem 2. (a) Show that every group of order 15 is isomorphic to $\mathbb{Z}_{15}$.

$|G| = 15 = 3 \cdot 5$. By Sylow III, it follows that $n_3 = 1$ and $n_5 = 1$. Thus, the Sylow p-subgroups of G are unique (and hence normal) and thus by an in-class proposition we get that G is isomorphic to $P_1 \times P_2$ where P_1 is the 3-Sylow subgroup and P_2 is the 5-Sylow subgroup. Furthermore, the orders of P_1 and P_2 are prime, so they must both be cyclic, so $G \cong P_1 \times P_2 \cong C_3 \times C_5 \cong C_{15}$ (by (1)). Thus, every group of order 15 is cyclic. □

(b) Let G be a group of order 255. Show that G has a normal subgroup H of order 17.

$|G| = 255 = 3 \cdot 5 \cdot 17$. So, $n_{17} \in \{1, 18, ...\} \cap \{1, 3, 5, 15\} \implies n_{17} = 1$. By the first Sylow theorem, this unique 17-Sylow subgroup will have order 17 and by our corollary to the second Sylow theorem this subgroup will be normal in G. □

(c) Show that G/H is cyclic.

Consider $|G/H| = [G : H] = \frac{|G|}{|H|} = \frac{255}{17} = 15 = 3 \cdot 5$. Then, by part a, we have that G/H is cyclic. □

(d) Show that G has a normal subgroup K of order either 3 or 5.

By Sylow III, $n_3 \in \{1, 4, 7, 10, 13, 16, 19, \dots, 85, \dots\} \cap \{1, 5, 17, 85\} \implies n_3 \in \{1, 85\}$. Similarly, $n_5 \in \{1, 6, 11, 16, 21, 26, \dots, 51, \dots\} \cap \{1, 3, 17, 51\} \implies n_5 \in \{1, 51\}$. Suppose that $n_5 = 51, n_3 = 85$. Then, we may use homework 5 problem 3.2 because the orders of all these subgroups are prime. So, as in 3.3, we have that G must contain $51(5 - 1) = 204$ elements of order 5 and $85(3 - 1) = 170$ elements of order 3. Their sum is more than the size of the group, so we have a contradiction. Thus either $n_5 = 1$ or $n_3 = 1$. Thus, by the first Sylow theorem and the corollary to the second Sylow theorem we have that there exists a (3 or 5)-Sylow subgroup that is normal in G and has order 3 or 5, respectively. □

(e) Show that, in either case, G/K is Abelian.

We have two cases:

$$|G/K| = \frac{|G|}{|K|} = \frac{255}{3 \text{ or } 5} = 85 \text{ or } 51.$$

In the first case, $n_5 \in \{1, 6, 11, 16, \dots\} \cap \{1, 17\}$, $n_{17} \in \{1, 18, \dots\} \cap \{1, 5\} \implies n_5 = 1$ and $n_{17} = 1$. Notice that $85 = 5 \cdot 17$ and $51 = 17 \cdot 3$. Thus, G/K has unique Sylow p-subgroups, and so we can apply an in-class proposition to obtain that $G/K \cong P_1 \times P_2 \cong C_5 \times C_{17} \cong C_{85}$. Since every cyclic group is Abelian, we have that G/K is Abelian. In the second case, observe that $n_3 = 1, n_{17} = 1$, and the same argument yields the desired result. □

(f) BONUS: Show that G is Abelian.

We have that G/K and G/H are both Abelian groups. Then by Problem 8.3, $G/(H \cap K)$ is also Abelian. Recall that $|H| = 17$, which is coprime to both 3 and 5, so Lagrange's theorem demands that

$$|H \cap K| = 1 \implies \frac{G}{H \cap K} \cong G,$$

which must then be Abelian. □

Problem 3. Let A_4 be the group of even permutations of the set $\{1, 2, 3, 4\}$. Consider the subgroups $H = \langle (123) \rangle$ and $K = \langle (12)(34), (13)(24) \rangle$.

(a) The left cosets of H are:

- $H = \{(), (123), (132)\}$,
- $(12)(34)H = \{(12)(34), (143), (243)\}$,
- $(13)(24)H = \{(13)(24), (142), (234)\}$,
- $(14)(23)H = \{(14)(23), (124), (134)\}$.

The right cosets of H are:

- $H = \{(), (123), (132)\}$,
- $H(12)(34) = \{(12)(34), (134), (234)\}$,
- $H(13)(24) = \{(13)(24), (124), (243)\}$,
- $H(14)(23) = \{(14)(23), (142), (143)\}$.

(b) H is a cyclic group of order 3, and so $H \cong \mathbb{Z}_3$. Its index in A_4 is $12/3 = 4$, which agrees with the number of left and right cosets. The left and right cosets of H are not the same, and so H is not a normal subgroup of A_4.

(c) The left cosets of K are:

- $K = \{(), (12)(34), (13)(24), (14)(23)\}$,
- $(123)K = \{(123), (134), (142), (243)\}$,
- $(132)K = \{(124), (132), (143), (234)\}$.

The right cosets of K are:

- $K = \{(), (12)(34), (13)(24), (14)(23)\}$,
- $K(123) = \{(123), (134), (142), (243)\}$,
- $K(132) = \{(124), (132), (143), (234)\}$.

(d) K is a group of order 4, and in fact $K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Its index in A_4 is $12/4 = 3$, which agrees with the number of left and right cosets. The left and right cosets of K coincide, and so K is a normal subgroup of A_4.

(e) Since $\gcd(|H|, |K|) = 1$, we have $H \cap K = \{()\}$, the trivial subgroup of A_4, which of course is a normal subgroup.

(f) The (internal) product HK has $3 \cdot 4 = 12$ elements, and so it coincides with A_4, which of course is a normal subgroup of itself.

(g) We have $H \times K = \mathbb{Z}_3 \times (\mathbb{Z}_2 \times \mathbb{Z}_2)$, which is an abelian group of order 12, isomorphic to $\mathbb{Z}_6 \oplus \mathbb{Z}_2$. (Note: Although $H \cap K = \{e\}$ and $|HK| = |H \times K|$, we still have $HK \ncong H \times K$. The reason is that the Decomposition Theorem does not apply here: H is not a normal subgroup, and H and K do not commute.)

Problem 4. Let Q_8 be quaternion group of order 8. Consider the left action of Q_8 on itself, and let $\varphi\colon Q_8 \to \mathrm{Sym}(Q_8) = S_8$ be the corresponding homomorphism, given by $\varphi(g)(x) = gx$. For every $x \in Q_8$, the stabilizer subgroup is the trivial subgroup $\{e\}$. Thus, the kernel of φ, which equals the intersection of all the stabilizer subgroups, is also equal to $\{e\}$. This shows that φ is injective (that is, the action is faithful), and thus Q_8 is isomorphic to $\varphi(Q_8)$, a subgroup of S_8. (By a small abuse of language, we simply say Q_8 is a subgroup of S_8.) An explicit realization of Q_8 as a subgroup of S_8 is obtained by sending $i \mapsto (1,2,4,6)(3,8,7,5)$ and $j \mapsto (1,3,4,7)(2,5,6,8)$, and thus $k \mapsto (1,5,4,8)(2,7,6,3)$.

We now consider the question whether Q_8 is a subgroup of S_5. We have that $|S_5| = 120 = 8 \cdot 3 \cdot 5$, and so, by Sylow I, S_5 must have a 2-Sylow subgroup of order 8. The dihedral group D_4 acts faithfully on the 4 vertices of a square, and thus is a subgroup of S_4, hence a subgroup of S_5. But $|D_4| = 8$, and so D_4 is a 2-Sylow subgroup of S_5. On the other hand, $Q_8 \ncong D_4$ (for instance, because Q_8 has 6 elements of order 4, whereas D_4 has only 2 such elements). Thus, Q_8 cannot be a 2-Sylow subgroup of S_5 (since all such subgroups are conjugate by Sylow II, and hence isomorphic). Therefore, Q_8 cannot be a subgroup of S_5 (since it is a 2-group of order 8, so it would be a 2-Sylow subgroup of S_5 if it were a subgroup of S_5).

Here is an alternate proof, which shows that, in fact, Q_8 is not a subgroup of S_6 or S_7, either, thereby proving that the embedding of Q_8 into S_8 guaranteed by Cayley's method from above is best possible. So suppose there is an injective homomorphism $Q_8 \to S_7$, i.e., a faithful action of Q_8 on the set $\{1, \ldots, 7\}$. By the Orbit-Stabilizer theorem, the index of each stabilizer equals the size of the corresponding orbit, and thus is at most 7; hence, none of the stabilizers is trivial. On the other hand, the center $Z(Q_8) = \{\pm 1\}$ is contained in any non-trivial subgroup of Q_8. Hence, the intersection of all the stabilizers contains $Z(Q_8)$, and so is non-trivial, thereby contradicting the faithfulness of the action. This proves $Q_8 \not\leq S_7$, and thus $Q_8 \not\leq S_n$ for any $n \leq 7$.

Problem 5. (a) Let G be a group of order $36 = 4 \cdot 9$, and let $n_p = \left|\mathrm{Syl}_p(G)\right|$ for $p \mid |G|$. We then have $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 4$; thus, $n_3 = 1$ or 4. Let's consider each case in turn.

First suppose $n_3 = 1$. Then there is a unique 3-Sylow subgroup of G, call it P, which must be a normal subgroup by Sylow II. Moreover, $|S| = 9$ is neither 1 nor 36, and so P is a non-trivial, proper, normal subgroup of G, thereby showing that G is not a simple group.

Now suppose $n_3 = 4$. By Sylow II, the conjugation action of G on $\mathrm{Syl}_3(G)$ is transitive; let $\varphi\colon G \to S_4$ be the corresponding homomorphism. Since $|G| = 36 > 24 = |S_4|$, the map φ cannot be injective. Thus, the normal subgroup $K = \ker(\varphi)$ is neither trivial (by non-injectivity of φ), nor equal to G (by transitivity of the action). Therefore, G is not simple. □

(b) Now let G be a group of order $56 = 8 \cdot 7$. We then have $n_7 \equiv 1 \pmod 7$ and $n_7 \mid 8$, implying

$n_7 = 1$ or 8. Let's consider each case in turn.

If $n_7 = 1$, then G has a single 7-Sylow subgroup, which must be normal by Sylow II, and so G is not simple.

If $n_7 = 8$, then G has 8 7-Sylow subgroups, which must all be cyclic of order 7, implying that G has $8 \cdot (7-1) = 48$ elements of order 7 in all. This leaves 8 other elements in G (including the identity), and by Sylow I, those 8 elements must comprise a 2-Sylow subgroup, which perforce must be the only one of this sort, and thus a normal subgroup. Hence, once again, G is not simple. □

Problem 6. We need to classify up to isomorphism all the finite groups G which satisfy the following two conditions: (1) G is a factor group of $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$, and (2) The order of every element of G divides 24. To start with, note the following:

(i) G is abelian (since it is a quotient of $\mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z}$, an abelian group).

(ii) G is generated by at most 2 elements (since it is a quotient of $\mathbb{Z}^2$, which can be generated by 2 elements, say, $(1,0)$ and $(0,1)$).

(iii) For every $x \in G$, we have $24x = 0$ (since $o(x) \mid 24$).

(iv) G is finite (by assumption, or as a consequence of the previous three properties).

By the classification of finite abelian groups, up to isomorphism the group G must be of the form

$$G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_s},$$

where $n_2 \mid n_1, n_3 \mid n_2, \ldots n_s \mid n_{s-1}$. By condition (i), we may have at most two factors in such a decomposition, i.e., $G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, with $n_2 \mid n_1$. (If $n_2 = 1$, we simply write $G = \mathbb{Z}_{n_1}$, and if $n_1 = 1$, we write $G = \{0\}$, the trivial group.) Moreover, by condition (iii), we must have $n_1 \mid 24$, and so $n_1 \in \{1, 2, 3, 4, 6, 8, 12, 24\}$. Thus, G must be precisely one of the 30 groups from the following table:

n_1	G							
1	$\{0\}$							
2	$\mathbb{Z}_2$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$						
3	$\mathbb{Z}_3$	$\mathbb{Z}_3 \oplus \mathbb{Z}_3$						
4	$\mathbb{Z}_4$	$\mathbb{Z}_4 \oplus \mathbb{Z}_2$	$\mathbb{Z}_4 \oplus \mathbb{Z}_4$					
6	$\mathbb{Z}_6$	$\mathbb{Z}_6 \oplus \mathbb{Z}_2$	$\mathbb{Z}_6 \oplus \mathbb{Z}_3$	$\mathbb{Z}_6 \oplus \mathbb{Z}_6$				
8	$\mathbb{Z}_8$	$\mathbb{Z}_8 \oplus \mathbb{Z}_2$	$\mathbb{Z}_8 \oplus \mathbb{Z}_4$	$\mathbb{Z}_8 \oplus \mathbb{Z}_8$				
12	$\mathbb{Z}_{12}$	$\mathbb{Z}_{12} \oplus \mathbb{Z}_2$	$\mathbb{Z}_{12} \oplus \mathbb{Z}_3$	$\mathbb{Z}_{12} \oplus \mathbb{Z}_4$	$\mathbb{Z}_{12} \oplus \mathbb{Z}_6$	$\mathbb{Z}_{12} \oplus \mathbb{Z}_{12}$		
24	$\mathbb{Z}_{24}$	$\mathbb{Z}_{24} \oplus \mathbb{Z}_2$	$\mathbb{Z}_{24} \oplus \mathbb{Z}_3$	$\mathbb{Z}_{24} \oplus \mathbb{Z}_4$	$\mathbb{Z}_{24} \oplus \mathbb{Z}_6$	$\mathbb{Z}_{24} \oplus \mathbb{Z}_8$	$\mathbb{Z}_{24} \oplus \mathbb{Z}_{12}$	$\mathbb{Z}_{24} \oplus \mathbb{Z}_{24}$

Remark: Any other group which satisfies the hypothesis of this problem must be isomorphic to one of the groups on this table. For instance, $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$, $\mathbb{Z}_8 \oplus \mathbb{Z}_6 \cong \mathbb{Z}_{24} \oplus \mathbb{Z}_2$, $\mathbb{Z}_6 \oplus \mathbb{Z}_4 \cong \mathbb{Z}_{12} \oplus \mathbb{Z}_2$, $\mathbb{Z}_{12} \oplus \mathbb{Z}_8 \cong \mathbb{Z}_{24} \oplus \mathbb{Z}_4$, etc.

Remark: Note that the above list coincides with the list of subgroups of $\mathbb{Z}_{24} \oplus \mathbb{Z}_{24}$.

Problem 7. Consider the group $G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{Z}_5, a \neq 0 \right\}$.

(a) The group G has order $20 = 4 \cdot 5$, so it has Sylow 2- and 5-subgroups, of orders 4 and 5, respectively. By Sylow III, $n_2 \equiv 1 \pmod 2$ and $n_2 \mid 5$, implying $n_2 = 1$ or 5. Likewise, $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 2$, implying $n_5 = 1$.

We start with the 2-Sylow subgroups. First note that $\mathbb{Z}_5^\times = \{1, 2, 3, 4\}$ is a cyclic group of order 4, generated by either 2 or 3. Thus, G has a Sylow 2-subgroup, call it P, generated by the diagonal matrix $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$, and this group is isomorphic to $\mathbb{Z}_4$. The subgroup P is not normal, but rather, it has 5 distinct conjugates, obtained by conjugating P by the 5 matrices of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ with $b \in \mathbb{Z}_5$. The complete list of Sylow 2-subgroups, then, is:

$$\mathrm{Syl}_2(G) = \left\{ \left\langle \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 2 & 4 \\ 0 & 1 \end{pmatrix} \right\rangle \right\}.$$

None of these subgroups is normal, but rather, G acts transitively on $\mathrm{Syl}_2(G)$ by permuting these subgroups, as predicted by Sylow II.

Now on to the 5-Sylow subgroups. One such subgroup is the subgroup Q generated by the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Clearly, $Q \cong \mathbb{Z}_5$, and by the above discussion (based on Sylow III), we know Q must be a normal subgroup.

(b) Is G a direct product of all its Sylow subgroups? As proven in class, if all Sylow subgroups of a group G are normal, then G is the product of its Sylow subgroups. But we did not prove the converse, so we must analyze this question more carefully, to see if the converse is true, at least in this case.

There are two ways to interpret this question. The straightforward way is to interpret it literally, that is, to decide whether

$$G \cong \prod_{P \in \mathrm{Syl}(G)} P = \prod_{\substack{p \mid |G| \\ p \text{ prime}}} \prod_{P \in \mathrm{Syl}_p(G)} P.$$

In general, if one of the p-Sylows is not normal, i.e., $n_p(G) > 1$, then the order of the group on the right side is at least $n_p \cdot |G|$, which is greater than the order of G. Thus, the (literal) converse to this statement indeed holds. For instance, in our case, the left side has order $|G| = 20$, whereas the right side has order $(5 \cdot 4) \cdot (1 \cdot 5) = 100$, so the answer to the question is an emphatic no.

The other (more subtle) way to interpret this question is whether the given group G is isomorphic to the direct product of p-Sylow subgroups, where p runs through the primes dividing $|G|$ as before, but with only a single p-Sylow chosen for each such prime (it does not matter which one is chosen, since they are all conjugate by Sylow II, and thus, all isomorphic). In other words, we must decide whether, across all p prime dividing $|G|$,

$$G \cong \prod_{P \in \mathrm{Syl}_p(G)/\sim} P,$$

where $\sim$ denotes the conjugacy relation, and where $\mathrm{Syl}_p(G)/\sim$ consists of a single equivalence class (by Sylow II), from which a representative P is chosen. Now this is a harder

question to answer, since the groups on both sides have the same order. In the problem at hand, then, the modified question asks whether G is isomorphic to $P \times Q$. And the answer is yet again an emphatic no, since G is non-abelian (for otherwise G would not have a non-normal subgroup such as P!), whereas $P \times Q = \mathbb{Z}_4 \times \mathbb{Z}_5 = \mathbb{Z}_{20}$ is abelian.

Problem 8. Let G be a group and $A, B \subseteq G$ be arbitrary subsets. Then we define

$$[A, B] := \langle [a, b] \mid a \in A, b \in B \rangle$$

to be the subgroup generated by commutators between A and B. In this notation, the derived (commutator) subgroup may be expressed as $G' = [G, G]$. Similarly, $A' = [A, A]$ refers to the set of commutators of an arbitrary subset $A \subseteq G$.

(1) Show that $H \trianglelefteq G$ if and only if $[G, H] \leq H$.

Proof. The "only if" will be considered the forward implication while the "if" will be backward.

($\Longrightarrow$) : Suppose that $H \trianglelefteq G$ so that for all $g \in G$ and $h \in H$, we have

$$ghg^{-1} \in H \implies [g, h] = ghg^{-1}h^{-1} \in H \implies [G, H] \leq H.$$

($\Longleftarrow$) : Suppose that $[G, H] \leq H$ so that for all $g \in G$ and $h \in H$, there exists $h_1 \in H$ such that

$$[g, h] = ghg^{-1}h^{-1} = h_1 \implies ghg^{-1} = h_1 h \in H \implies H \trianglelefteq G.$$

□

(2) Prove that $K' \trianglelefteq G$ whenever $K \trianglelefteq G$.

Proof. We will make use of the fact that commutator subgroups are *characteristic* (proven below), which is to say that they are preserved under all automorphisms of the group they are defined within, not only inner automorphisms. The argument used for this proof may be applied to show that if $H \trianglelefteq K \trianglelefteq G$ and H is characteristic in K, then $H \trianglelefteq G$.

Let $\sigma^a : G \to G$ be the inner automorphism defined as conjugation by any given $a \in G$. By hypothesis, $K \trianglelefteq G$ so that the restriction $\sigma^a|_K \in \mathrm{Aut}(K)$. Because $K' \trianglelefteq K$ is characteristic, the further restriction $\sigma^a|_{K'} \in \mathrm{Aut}(K')$. Because the choice of $a \in G$ was unrestricted, we conclude that all inner automorphisms of G restricted to K' have image K'; that is to say $K' \trianglelefteq G$.

Commutator subgroups are characteristic: Let $\Phi \in \mathrm{Aut}(G)$ be any automorphism and $g_1, g_2 \in G$ be any pair of elements. Because G' is the subgroup generated by commutators of elements and because there is a bijective correspondence between G' and $\Phi(G')$, it suffices to show that Φ takes commutators to commutators. A generic commutator $[g_1, g_2] \in G'$ may then be written as

$$[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1} \implies \Phi([g_1, g_2]) = \Phi(g_1)\Phi(g_2)\Phi(g_1)^{-1}\Phi(g_2)^{-1} = [\Phi(g_1), \Phi(g_2)] \in G',$$

where all that was used were properties of homomorphisms. Therefore, the restriction $\Phi|_{G'} \in \mathrm{Aut}(G')$, so G' is characteristic in G. □

(3) If $H, K \trianglelefteq G$ such that G/H and G/K are Abelian, show that $G/(H \cap K)$ is also Abelian.

Proof. Here we will make use of the universal property of commutator subgroups; namely, G/N is Abelian if and only if $G' \leq N$. By hypothesis, both H and K produce Abelian quotients, so $G' \leq H \cap K$. Invoking the fact that intersections of normal subgroups are again normal, we may immediately apply the universal property to conclude that $G/(H \cap K)$ is Abelian. □

(4) BONUS: If $|G'| = m$ then each element $x \in G$ has at most m conjugates.

Proof. Let $x^g := gxg^{-1}$ denote the conjugate of x by g, for any given $x, g \in G$. Observe that

$$x^g x^{-1} = [g, x] \in G' \implies G'x^g = G'x \implies Cl(x) \subseteq G'x \implies |Cl(x)| \leq \left|G'x\right| = \left|G'\right|.$$

By hypothesis $|G'| = m$, so we immediately see that $|Cl(x)| \leq m$ as desired. □

Problem 9. We call a group homomorphism $\varphi\colon G \to H$ a *monomorphism* if $\varphi \circ f = \varphi \circ g \implies f = g$ for homomorphisms f, g. Dually, we call a homomorphism $\psi : G' \to H'$ an *epimorphism* if $f' \circ \psi = g' \circ \psi \implies f' = g'$ for any homomorphisms f', g'. Show that monomorphisms are injective and that epimorphisms are surjective.

Proof. We will first confront the issue of injectivity and follow with surjectivity.

(1) Denote by $K = \mathrm{Ker}(\varphi)$ the kernel of the homomorphism $\varphi\colon G \to H$. Then K is a (normal) subgroup of G. We may define homomorphisms $f, g\colon K \to G$ via the mappings

$$f(k) = e \quad \text{and} \quad g(k) = k$$

for all $k \in K$. Clearly $\varphi \circ f$ is the trivial map because all homomorphisms preserve the identity. On the other hand, $\varphi(k) = e$ for all $k \in K$, so $\varphi \circ g$ is also a trivial map due to the fact that $\mathrm{Im}(g) = K$. Because φ is a monomorphism,

$$\varphi \circ f = \varphi \circ g \implies f = g \implies \mathrm{Im}(f) = \mathrm{Im}(g) = \{e\} = K.$$

Because $K = \mathrm{Ker}(\varphi)$ is the trivial group, φ is injective.

(2) Denote by I the image $\mathrm{Im}(\psi)$ and by S the factor <u>set</u> H'/I. Let us define group actions $f', g'\colon H' \times S \to S$ via the mappings

$$f'(h, aI) = aI \quad \text{and} \quad g'(h, aI) = ah^{-1}I$$

for any $a, h \in H'$ (check that these are indeed group actions). Through abuse of notation, we conflate the group actions with their permutation reprsentations $f', g'\colon H' \to \mathrm{Sym}(S)$. In particular, f' is a trivial homomorphism because every element of S is fixed by all of H'. By our definition of g', observe that

$$\mathrm{Im}(g' \circ \psi) = g'(I) = \{\mathbb{1}_S\} = \mathrm{Im}(f' \circ \psi)$$

is the trivial group. It is clear that homomorphisms sharing domain and codomain with trivial image are equal. Now because ψ is epic

$$f' \circ \psi = g' \circ \psi \implies f' = g' \implies aI = ah^{-1}I \implies \left(ah^{-1}\right)^{-1} a = ha^{-1}a = h \in I$$

for all $a, h \in H'$. In particular, $H' \leq I \implies H' = I$; i.e., ψ is surjective.

□