Math 453

Selected Solutions to Assignment 7

Problem 3: Let $f : G \to H$ be a homomorphism of groups. Let $\ker(f) := \{g \in G | f(g) = e\}$ where $e \in H$ is the identity of H. Show that $\ker(f)$ is a subgroup of G.

Solution: To show that $\ker(f)$ is a subgroup, we must show that the identity e_G on G is in $\ker(f)$; that $\ker(f)$ is closed under the group operation on G; and that for each $a \in \ker(f)$, the inverse of a in G, a^{-1}, is in $\ker(f)$. First, observe that since f is a homomorphism, we have $f(e_G) = e$, so $e_G \in \ker(f)$. Now, let $a, b \in \ker(f)$; again since f is a homomorphism, we have $f(ab) = f(a)f(b) = ee = e$, so $ab \in \ker(f)$. Finally, note that $e = f(e_G) = f(a^{-1}a) = f(a)f(a^{-1}) = ef(a^{-1}) = f(a^{-1})$, so $a^{-1} \in \ker(f)$. Therefore, $\ker(f)$ is a subgroup of G.

Problem 10: (Note: this statement is incorrect the way it is stated. The correct statement should be "Prove that a group G has exactly 3 subgroups if and only if G is cyclic with $|G| = p^2$ for a prime number p.") Prove that if a group G has exactly 3 subgroups, then $|G| = p^2$ for a prime number p.

Solution: Suppose G has exactly 3 subgroups, so G has as subgroups exactly the trivial subgroup $\langle e \rangle$; G itself; and one proper, nontrivial subgroup $H \subsetneq G$. Thus, there exists an element $g \in G \setminus H$; in particular, $g \neq e$, so $\langle g \rangle \neq \langle e \rangle$. Since $g \notin H$, we have $\langle g \rangle \neq H$. Hence, we have $\langle g \rangle = G$, so G is cyclic with generator g. Now, if $\big|\langle g \rangle\big| = \infty$, we have that $G \cong \mathbb{Z}$; since $\langle k \rangle$ is a distinct subgroup of $\mathbb{Z}$ for each $k \in \mathbb{N}$, this contradicts the fact that G has exactly one proper nontrivial subgroup. Hence, $\big|\langle g \rangle\big| = n$ for some $n \in \mathbb{N}$. Now, let $n = \prod_{i=1}^{m} a_i^{\alpha_i}$ for $\alpha_i \in \mathbb{N}$ and distinct prime $a_i \in \mathbb{N}$. If $m > 1$, since G is cyclic, there exist at least two nontrivial proper subgroups of G with orders a_1 and a_2, respectively; this contradicts the fact that G has exactly one proper nontrivial subgroup. Hence, $|G| = p^\alpha$. Again since G is cyclic, for each $1 \leq i \leq \alpha - 1$, there exists a (distinct) nontrivial proper subgroup of order p^i. Thus, $\alpha = 2$, so $|G| = p^2$.

Problem 20: Let G be a group, and let $a \in G$. Consider the map $I_a : G \to G$ given by $I_a(g) := aga^{-1}$. Show that I_a is an automorphism of G.

Solution: To show that I_a is an automorphism of G, we must show that it is a homomorphism; that it is surjective; and that it is injective. Let

$g, h \in G$; then $I_a(gh) = agha^{-1} = aga^{-1}aha^{-1} = I_a(g)I_a(h)$, so I_a is a homomorphism. Furthermore, let $k \in G$; then $I_a(a^{-1}ka) = aa^{-1}kaa^{-1} = k$, so I_a is surjective. Finally, suppose $I_a(g) = I_a(h)$; then $aga^{-1} = aha^{-1}$, so multiplying on the left by a^{-1} and on the right by a, we get $g = h$, so I_a is injective. Therefore, I_a is an automorphism of G.