$12+13=25$

MAT 511 **HW #2** Name SOLUTIONS

9/7/13, due Friday 9/13/13

25 points

3 1. Let G be a group and $g \in G$. Let $\rho_g : G \to G$ and $\lambda_g : G \to G$ be the functions defined by $\rho_g(x) = xg$ and $\lambda_g(x) = gx$ for $x \in G$. The functions $\rho: G \to S_G$, $g \mapsto \rho_g$ and $\lambda: G \to S_G$, $g \mapsto \lambda_g$ are injective homomorphisms. Let $R = \operatorname{im}(\rho) \subseteq S_G$ and $L = \operatorname{im}(\lambda) \subseteq S_G$ denote the images of ρ and λ, respectively. Each of these subgroups is isomorphic to G - that is Cayley's Theorem. Show that R is equal to the centralizer of L in the group S_G.[1]

Let $\varphi \in L$ and $\psi \in R$. Then $\varphi = \lambda_g$ and $\psi = \rho_h$ for some $g, h \in G$. Then $\varphi \circ \psi(x) = \lambda_g \circ \rho_h(x) = \lambda_g(xh) = g(xh)$ $= (gx)h = \rho_h(gx) = \rho_h \circ \lambda_g(x) = \psi \circ \varphi(x)$. Thus $R \subseteq \mathbf{C}_G(L)$. Conversely, suppose $\psi \in S_G$ and ψ centralizes L, that is, $\psi \circ \lambda_g = \lambda_g \circ \psi$ for all $g \in G$. Let $h = \psi(e_G)$. Claim $\psi = \rho_h$. Indeed, $\psi(x) = \psi(x \cdot e_G) = \psi \circ \lambda_x(e_G) = \lambda_x \circ \psi(e_G) = \lambda_x(\psi(e_G))$ $= \lambda_x(h) = xh = \rho_h(x)$, for all $x \in G$. Since $\psi = \rho_h$, $\psi \in R$. Thus $\mathbf{C}_{S_G}(L) = R$.

3 2. Do Problem 1.36 from the text. Suppose $f : G \to G$ is an automorphism satisfying $f \circ f = id_G$ and $f(x) = x \implies x = e$ $\forall x \in G$. Claim: Every $g \in G$ can be written $g = x^{-1}f(x)$ for some $x \in G$. Proof: Consider $\varphi : G \to G$ defined by $\varphi(x) = x^{-1}f(x)$. Then φ is injective - indeed, if $\varphi(x) = \varphi(y)$, then $x^{-1}f(x) = y^{-1}f(y)$, which implies $f(x)f(y)^{-1} = xy^{-1}$, hence $f(xy^{-1}) = xy^{-1}$, which implies $xy^{-1} = e$, so $x = y$. Since φ is injective and G is finite, φ is a bijection. This proves the claim. Then, since $f \circ f = id_G$, if $u \in G$, $u = x^{-1}f(x)$, and then $f(u) = f(x^{-1})f(f(x)) = f(x)^{-1}x = (x^{-1}f(x))^{-1}$ $= u^{-1}$. Since $f: G \to G$ is a homomorphism and

[1] Recall: the *centralizer* of a subgroup H in a group K is $\mathbf{C}_K(H) := \{x \in K \mid xh = hx \text{ for all } h \in H\}$.

$f(u) = u^{-1}$ for all $u \in G$, G is abelian. Indeed $uv = (u^{-1})^{-1}(v^{-1})^{-1} = f(u^{-1})f(v^{-1}) = f(u^{-1}v^{-1}) = f((vu)^{-1})$ $= vu$. $\square$

3 3. Let G be a group. An element $g \in G$ is called a *nongenerator* if, for any $X \subseteq G$, if $\langle X \cup \{g\} \rangle = G$, then $\langle X \rangle = G$. A subgroup M of G is *maximal* if M is proper and, for any proper subgroup H of G, if $M \subseteq H \subseteq G$ with H a proper subgroup of G, then $H = M$.

Show that the set of nongenerators of G is equal to the intersection $\Phi(G)$ of all maximal subgroups of G. ($\Phi(G)$ is called the *Frattini subgroup* of G.)

Let $g \in \Phi(G)$. Suppose g is not a non-generator. Then $\exists X \subseteq G$ such that $\langle X \cup \{g\} \rangle = G$ but $\langle X \rangle \neq G$. Since $\langle X \rangle$ is a proper subgroup of G and $|G| < \infty$, there is a maximal subgroup M of G with $\langle X \rangle \subseteq M$. (This can be proved by induction on the index $|G : \langle X \rangle|$.) Since $g \in \Phi(G)$, $g \in M$ as well. Then $\langle X \cup \{g\} \rangle \subseteq M$, a contradiction since M is proper. Thus g is a non-generator. Conversely, suppose g is a non-generator and let M be a maximal subgroup. Suppose $g \in M$. Then $\langle M \cup \{g\} \rangle \supsetneq M$, so $\langle M \cup \{g\} \rangle = G$ by maximality of M.

Then $\langle M \rangle = G$ since g is a non-generator. But $\langle M \rangle = M$ because $M \leq G$. Then $M = G$, a contradiction. Thus $g \in M$. Since M was arbitrary, $g \in \Phi(M)$.

3 4. Suppose G is a finite group having a unique maximal subgroup. Prove $|G|$ is a power of a prime.

Let M be the unique maximal subgroup of G. Then $M \neq G$. Let $x \in G - M$, and consider $\langle x \rangle$. If $\langle x \rangle$ is a proper subgroup, then $\langle x \rangle$ is contained in a maximal subgroup (since G is finite), which must be M, since M is unique. Since $x \notin M$, this cannot be. Thus $\langle x \rangle = M$, so M is cyclic. x has finite order since G is finite. Let $|x| = n$ and suppose p and q are distinct primes dividing n.

Let $M = \langle x^p \rangle$ and $N = \langle x^q \rangle$. Then $|G:M| = p$ and $|G:N| = q$ are prime, which implies M and N are maximal by Lagrange's Theorem. Then $M = N$, a contradiction. Then $|G| = p^n$ for some prime p.