**HOMEWORK 5 SOLUTIONS**

1. Let $S \subseteq G$, where $G$ is a group. Define the centralizer of $S$ to be $C_G(S) = \{ g \in G \mid gs = sg \ \forall s \in S \}$ and the normalizer of $S$ to be $N_G(S) = \{ g \in G \mid gS = Sg \}$.

   - i) Show that $C_G(S)$ and $N_G(S)$ are subgroups of $G$.
   - ii) Show that if $H \subseteq G$, then $H \trianglelefteq N_G(H)$ and $N_G(H)$ is the largest such subgroup of $G$, i.e. if $H \trianglelefteq G' \leq G$, then $G' \leq N_G(H)$.
   - iii) Show that if $H \subseteq G$, then $C_G(H) \trianglelefteq N_G(H)$. What if $H$ is only a subset of $G$ (not necessarily a subgroup)?

**Proof.**

   - i) We first show $C_G(S) \leq G$. Clearly, $e \in C_G(S)$ since $es = s = se$ for all $s \in S$. Suppose $x, y \in C_G(S)$. Then, for all $s \in S$, $(xy)(s) = x(y(s)) = (xys) = (xs)y = s(xy)$, i.e. $xy \in C_G(S)$. Similarly, since $x \in C_G(S)$, $x^{-1}s = (x^{-1}s)e = (x^{-1}s)(x^{-1}) = x^{-1}(sx)x^{-1} = x^{-1}(xs)x^{-1} = (x^{-1}x)(sx^{-1}) = xsx^{-1}$, and so $x^{-1} \in C_G(S)$. Therefore, $C_G(S) \leq G$.

   Now, we show $N_G(S) \leq G$. Again, $e \in N_G(S)$ since $eS = S = Se$. Suppose $x, y \in N_G(S)$. Then $xS = Sx$ and $yS = Sy$. Let $(xy)s \in (xy)S$. Then $ys \in yS = Sy$, and so $(xy)s = x(ys) = x(sy) = xy \in C_G(S)$. Similarly, since $xs' \in xS = Sx$, $(xs')y = (s''xy) \in S(xy)$ for some $s'' \in S$, i.e. $(xy)S \subseteq S(xy)$. A similar argument gives the reverse inclusion, and hence $(xy)S = S(xy)$, and so $xy \in N_G(S)$. Let $x^{-1}s \in x^{-1}S$. Then, since $x \in N_G(S)$, $xS = Sx$, and thus $sx = xs'$ for some $s' \in S$. Then

     $$x^{-1}s = (x^{-1}s)(x^{-1}) = x^{-1}(sx)x^{-1} = x^{-1}(xs)x^{-1} = (x^{-1}x)(sx^{-1}) = e(sx^{-1}) = s'x^{-1} \in Sx^{-1},$$

   and so $x^{-1}S \subseteq Sx^{-1}$. A similar argument gives the reverse inclusion, and hence $x^{-1}S = Sx^{-1}$, i.e. $x^{-1} \in N_G(S)$. Therefore, $N_G(S) \leq G$.

   - ii) Suppose $H \subseteq G$. By definition, $H \trianglelefteq N_G(H)$: for every $h \in H$, $hH = H = Hh$, and so $h \in N_G(H)$, i.e. $H \leq N_G(H)$. Moreover, for every $g \in N_G(H)$, $gH = Hg$, i.e. $H$ is normal in $N_G(H)$. Suppose $G' \leq G$ such that $H \trianglelefteq G'$. Then, for every $g' \in G'$, $g'H = Hg'$. Since $G' \leq G$, we must then have $g' \in N_G(H)$, and thus $G' \leq N_G(H)$, i.e. $N_G(H)$ is the largest subgroup of $G$ in which $H$ is normal.

   - iii) We will show that, in general, $C_G(S) \trianglelefteq N_G(S)$, regardless of whether or not $S$ is a subgroup of $G$. Let $c \in C_G(S)$. Then $ch = hc$ for all $h \in H$, and thus $cS = Sc$, so $c \in N_G(S)$. Thus, $C_G(S) \leq N_G(S)$. Let $n \in N_G(S)$, and $ncn^{-1} \in nC_G(S)n^{-1}$. Let $s \in S$. Then, since $n \in N_G(S)$, $sn = ns'$ for some $s' \in S$. Multiplying this equation on the left and right by $n^{-1}$ gives $n^{-1}s = s'n^{-1}$. Since $c \in C_G(S)$, $cs' = s'c$, and so
Thus, \( ncn^{-1} \in C_G(S) \), and so \( nC_G(S)n^{-1} \subseteq C_G(S) \) for all \( n \in N_G(S) \). Therefore, \( C_G(S) \trianglelefteq N_G(S) \).
44. Let $\phi : G \rightarrow G'$ be a group homomorphism. Show that if $G$ is finite, then $|\phi[G]|$ is finite and is a divisor of $|G|$.

Proof. Clearly, since $\phi$ is a function, $|\phi[G]| \leq |G|$, and is hence finite. We now show that not only does $|\phi[G]|$ divide $|G|$, but in fact $|G| = |\phi[G]| \cdot |\ker \phi|$; that is, $|\phi[G]| = (K : G)$. To show this, let $K = \ker \phi$, let $L_K$ be the set of left cosets of $K$ in $G$, and define the map $\Sigma : \phi[G] \rightarrow L_K$ by $\Sigma(\phi(g)) = gK$. We first show that $\Sigma$ is well defined. Suppose $x \in G$ such that $\phi(x) = \phi(g)$. Then, since $\phi$ is a group homomorphism, $\phi(g^{-1}x) = \phi(g^{-1})\phi(x) = \phi(g)^{-1}\phi(x) = \phi(g)^{-1}\phi(g) = e'$, and so $g^{-1}x \in K$. Then $x \in gK$, and so $xK = gK$. Thus, $\Sigma(\phi(x)) = xK = gK = \Sigma(\phi(g))$, and so $\Sigma$ is well defined. This argument in reverse shows that $\Sigma$ is injective. Since $\Sigma$ is clearly surjective since $\phi(g) \in \phi[G]$ for all $gK \in L_K$, $\Sigma$ is a bijection, as desired. Thus, $|\phi[G]| = |L_K| = (K : G)$, which divides $|G|$ by Lagrange’s Theorem.

45. Let $\phi : G \rightarrow G'$ be a group homomorphism. Show that if $G'$ is finite, then $|\phi[G]|$ is finite and is a divisor of $|G'|$.


47. Suppose $\phi : G \rightarrow G'$ is a group homomorphism. Show that if $|G|$ is prime, then either $\ker \phi = G$ or $\phi$ is injective.

Proof. By Problem 44, $|G| = |\phi[G]| \cdot |\ker \phi|$. Since $|G|$ is prime, either $|\ker \phi| = |G|$, in which case $\ker \phi = G$, or $|\ker \phi| = 1$, in which case $\ker \phi = \{e\}$, and hence $\phi$ is injective.

49. Show that if $\phi : G \rightarrow G'$ and $\psi : G' \rightarrow G''$ are group homomorphisms, then $\psi \circ \phi : G \rightarrow G''$ is a group homomorphism.

Proof. Let $a, b \in G$. Then, denoting our groups by $(G, \cdot)$, $(G', \star)$, and $(G'', \otimes)$, we have

$$\psi \circ \phi(a \cdot b) = \psi(\phi(a \cdot b)) = \psi(\phi(a) \star \phi(b)) = \psi(\phi(a)) \otimes \psi(\phi(b)) = \psi \circ \phi(a) \otimes \psi \circ \phi(b)$$

and hence $\psi \circ \phi$ is a group homomorphism.
50. Let $\phi : G \to H$ be a group homomorphism. Show that $\phi[G]$ is abelian if and only if $xyx^{-1}y^{-1} \in \ker \phi$ for all $x, y \in G$.

Proof.

($\Rightarrow$) Suppose $\phi[G]$ is abelian. Then, since $\phi$ is a group homomorphism, for any $x, y \in G$ we have

$$
\phi(xy^{-1}x^{-1}) = \phi(x)\phi(y)\phi(x^{-1})\phi(y^{-1}) = \phi(x)\phi(y) = \phi(x)\phi(x^{-1})\phi(y)\phi(y^{-1}) = e_H e_H = e_H
$$

Thus, $xy^{-1}x^{-1} \in \ker \phi$ for all $x, y \in G$.

($\Leftarrow$) Suppose $xy^{-1}x^{-1} \in \ker \phi$ for all $x, y \in G$. Then, for any $\phi(x), \phi(y) \in \phi[G], xy \in \ker \phi(xy)$, i.e. $xy = k(yx)$ for some $k \in \ker \phi$. Thus, since $\phi$ is a group homomorphism,

$$
\phi(x)\phi(y) = \phi(xy) = \phi(kyx) = \phi(k)\phi(yx) = e_H(\phi(y)\phi(x)) = \phi(y)\phi(x)
$$

i.e. $\phi[G]$ is abelian.

52. Let $\phi : G \to G'$ be a group homomorphism with kernel $K$. Show that $\phi^{-1} \phi(g) = gK$.

Proof. This follows from our argument in the proof of Problem 44:

$$
x \in \phi^{-1} \phi(g) \iff \phi(x) = \phi(g) \iff \phi(g^{-1}x) = e' \iff g^{-1}x \in K \iff x \in gK.
$$

53. Let $G$ be a group, $h, k \in G$, and define $\phi : \mathbb{Z} \times \mathbb{Z} \to G$ by $\phi(m, n) = h^mk^n$. Show that $\phi$ is a group homomorphism if and only if $hk = kh$.

Proof.

($\Rightarrow$) Suppose $\phi$ is a group homomorphism. Then

$$
hk = \phi(1, 1) = \phi((0, 1) + (1, 0)) = \phi(0, 1) \phi(1, 0) = kh
$$

($\Leftarrow$) Suppose $hk = kh$. Then, for all $(a, b), (m, n) \in \mathbb{Z} \times \mathbb{Z},$

$$
\phi((a, b) + (m, n)) = \phi(a + m, b + n) = h^{a+m}k^{b+n} = h^a k^b h^m k^n = \phi(a, b) \phi(m, n)
$$

i.e. $\phi$ is a group homomorphism.
Part III Section 14 Exercises

27 & 28. A subgroup $H \leq G$ is conjugate to a subgroup $K \leq G$ if there exists $g \in G$ such that $i_g[H] = K$. Prove that conjugacy is an equivalence relation on the collection of subgroups of $G$. Characterize the normal subgroups of $G$ in terms of this equivalence relation and its associated partition.

Proof. Let $H, K, M \leq G$. Since $ehe^{-1} = ehe = h$ for all $h \in H$, $i_e[H] = H$, and so $H$ is conjugate to itself, i.e. conjugacy is reflexive. Suppose $i_g[H] = K$. We will show that $H = i_{g^{-1}}[K]$. Let $h \in H$. Then, since $i_g[H] = K$, $ghg^{-1} = k$ for some $k \in K$. Then $h = g^{-1}kg = g^{-1}k(g^{-1})^{-1} \in i_{g^{-1}}K$, and so $H \subseteq i_{g^{-1}}[K]$. The same argument in reverse gives the reverse inclusion, and thus $H = i_{g^{-1}}[K]$, i.e. conjugacy is symmetric.

Now, suppose $i_g[H] = [K]$ and $i_y[K] = M$. We will show that $i_{yx}[H] = M$. Let $m \in M$. Then, since $i_y[K] = M$, $m = yky^{-1}$ for some $k \in K$. Similarly, since $i_x[H] = K$, $k = xhx^{-1}$ for some $h \in H$. Then $m = yky^{-1} = y(xhx^{-1})y^{-1} = (yx)h(x^{-1}y^{-1}) = (yx)h(yx)^{-1}$. Then $m \in i_{yx}[H]$, and so $M \subseteq i_{yx}[H]$. The same argument in reverse gives the reverse inclusion, and hence $i_{yx}[H] = M$, i.e. conjugacy is transitive.

Therefore, conjugacy is an equivalence relation on the collection of subgroups of $G$.

Since $N \leq G$ if and only if $i_g[N] = gNg^{-1} = N$ for all $g \in G$, the normal subgroups of $G$ are precisely the (representatives of the) single-element equivalence classes of the collection of subgroups of $G$ modulo conjugacy, i.e. the subgroups of $G$ such that $H$ is conjugate to $N$ if and only if $H = N$. ■

31. Show that the intersection of a collection of normal subgroups $\{N_\alpha \mid \alpha \in I\}$ of a group $G$ is itself a normal subgroup of $G$.

Proof. Let $g \in G$, and let $gng^{-1} \in g \bigcap_{\alpha \in I} N_\alpha g^{-1}$. Then, since $n \in \bigcap_{\alpha \in I} N_\alpha$, $n \in N_\alpha$ for all $\alpha \in I$. Then, since each $N_\alpha$ is normal in $G$, $gng^{-1} \in N_\alpha$ for all $\alpha \in I$. Then $gng^{-1} \in \bigcap_{\alpha \in I} N_\alpha$, and so $g \bigcap_{\alpha \in I} N_\alpha g^{-1} \subseteq \bigcap_{\alpha \in I} N_\alpha$. Therefore, $\bigcap_{\alpha \in I} N_\alpha \leq G$. ■

37. Let $G$ be a group. Show that $\text{Aut}(G)$ is a group under function composition, and show that $\text{Inn}(G) \subseteq \text{Aut}(G)$.

Proof. Clearly, the composition of bijections is itself a bijection. By Problem 49, the composition of group homomorphisms is also a group homomorphism. Thus, composition is a binary operation on $\text{Aut}(G)$. Since the identity map $\text{id}_G : G \rightarrow G$ defined by $\text{id}_G(g) = g$ is clearly an automorphism, and isomorphisms are invertible, $\text{Aut}(G)$ is a group under the usual function composition.
We now show that \( \text{Inn}(G) \trianglelefteq \text{Aut}(G) \). Since \( i_e(g) = ege^{-1} = ege = g \) for all \( g \in G \), \( \text{id}_G = i_e \in \text{Inn}(G) \).

Let \( i_x, i_y \in \text{Inn}(G) \). Then, for all \( g \in G \),
\[
i_x \circ i_y(g) = i_x(i_y(g)) = i_x(ygy^{-1}) = x(ygy^{-1})x^{-1} = (xyg)(y^{-1}x^{-1}) = (xy)(xy^{-1}) = i_{xy}(g)
\]

Thus, \( i_x \circ i_y = i_{xy} \in \text{Inn}(G) \). Similarly, \( (i_x)^{-1} = i^{-1}_x \in \text{Inn}(G) \) since
\[
i_x \circ i_{x^{-1}}(g) = x(x^{-1}g)x^{-1} = (x^{-1})g(x^{-1}) = ege = i_e(g) = ege = (x^{-1})g(x^{-1}x) = x^{-1}(xgx^{-1})x = i_{x^{-1}} \circ i_x(g)
\]

for all \( g \in G \). Thus, \( \text{Inn}(G) \trianglelefteq \text{Aut}(G) \). We now show that \( \text{Inn}(G) \) is normal in \( \text{Aut}(G) \). Let \( \phi \in \text{Aut}(G) \), and let \( \phi i_x \phi^{-1} \in \phi \text{Inn}(G) \phi^{-1} \).

Then, for all \( g \in G \), since \( \phi \in \text{Aut}(G) \),
\[
\phi i_x \phi^{-1}(g) = \phi(i_x(\phi^{-1}(g))) = \phi(\phi^{-1}(g)x^{-1}) = \phi(x)\phi(\phi^{-1}(g))\phi(x^{-1}) = \phi(x)g\phi(x)^{-1} = i_{\phi(x)}(g)
\]

and so \( \phi i_x \phi^{-1} = i_{\phi(x)} \in \text{Inn}(G) \), i.e. \( \phi \text{Inn}(G) \phi^{-1} \subseteq \text{Inn}(G) \). Therefore, \( \text{Inn} \trianglelefteq \text{Aut}(G) \).

\(39. \) Suppose \( H \trianglelefteq G, H' \trianglelefteq G' \), and \( \phi : G \to G' \) is a group homomorphism such that \( \phi[H] \subseteq H' \). Prove that \( \phi \) induces a group homomorphism \( \phi_* : G/H \to G'/H' \).

\textit{Proof.} Define \( \phi_* \) by \( \phi_*(gH) = \phi(g)H' \). We will first show that \( \phi_* \) is well defined. Suppose \( xH, yH \in G/H \) such that \( \phi_*(xH) = \phi_*(yH) \). Then \( \phi(x)H' = \phi(y)H' \). Then, since \( \phi \) is a homomorphism and by definition of the group \( G'/H' \),
\[
\phi(x^{-1}y)H' = \phi(x^{-1})\phi(y)H' = \phi(x)^{-1}\phi(y)H' = (\phi(x)H')^{-1}\phi(y)H' = H'
\]

and thus \( \phi(x^{-1}y) \in H' \). Then, since \( \phi[H] \subseteq H, x^{-1}y \in H \). Then \( y \in xH \), and thus \( yH = xH \). Therefore, \( \phi_* \) is well defined.

We now verify that \( \phi_* \) is a group homomorphism. For any \( aH, bH \in G/H \), since \( \phi \) is a homomorphism,
\[
\phi_*(aH bH) = \phi_*(ab H) = \phi(ab)H' = \phi(a)\phi(b)H' = \phi(a)H' \phi(b)H' = \phi_*(aH) \phi_*(bH),
\]

and so \( \phi_* : G/H \to G'/H' \) is a group homomorphism.
Challenge: Since \( \text{Inn}(G) \leq \text{Aut}(G) \) by Problem 37, we can define the quotient group \( \text{Out}(G) = \text{Aut}(G) / \text{Inn}(G) \). Describe \( \text{Out}(S_3) \).

Proof. We will first describe \( \text{Aut}(S_3) \). Since \( S_3 = \langle (12), (13), (23) \rangle \), \( \Theta \in \text{Aut}(S_3) \) is completely determined by \( \Theta(12), \Theta(13), \) and \( \Theta(23) \). In order for \( \Sigma \) to be an automorphism of \( S_3 \), we must have \( |\Theta(\lambda)| = |\lambda| \) for all \( \lambda \in S_3 \). In particular, \( \Theta \) must map transpositions to transpositions since the only elements of order 2 in \( S_3 \) are the transpositions (note that this portion of our argument does not hold in \( S_n \) for \( n \geq 3 \); the product of any number of disjoint transpositions also has order 2). In order to be bijective, \( \Theta \) must map each transposition to a unique transposition. Thus, we have 6 candidate functions, one for each possible permutation of the transpositions \( (12), (13), \) and \( (23) \), i.e. the functions \( \Xi = \text{id}_{S_3}, \Delta(12) = (13), \Delta(13) = (12), \Delta(23) = (23), \Lambda(12) = (23), \Lambda(13) = (13), \Lambda(23) = (12), \Sigma(12) = (12), \Sigma(13) = (23), \Sigma(23) = (13), \Phi(12) = (12), \Phi(13) = (23), \Phi(23) = (12), \) and \( \Psi(12) = (23), \Psi(13) = (12), \Psi(23) = (13) \). These functions are extended to isomorphisms of \( S_3 \) by requiring that the value of the function applied to a product of transpositions is exactly the product (in order) of the value of the function at the transpositions, i.e. \( C(\prod_{i=1}^{m} \tau_i) = \prod_{i=1}^{m} C(\tau_i) \) for each of our candidates \( C \), where each \( \tau_i \) is a transposition. As can be checked directly (recall that each \( \sigma \in S_3 \) can be written as a product of at most 2 transpositions by Homework 3 Problem 27), each of \( \Xi, \Delta, \Lambda, \Sigma, \Phi, \) and \( \Psi \) is in fact an automorphism of \( S_3 \), and so \( \text{Aut}(S_3) = \{ \Xi, \Delta, \Lambda, \Sigma, \Phi, \Psi \} \). Moreover, perhaps by labeling \( (12) = \tau_1, (13) = \tau_2, \) and \( (23) = \tau_3 \), we see that \( \Delta = (\tau_1 \tau_2), \Lambda = (\tau_1 \tau_3), \Sigma = (\tau_2 \tau_3), \Phi = (\tau_1 \tau_2 \tau_3), \) and \( \Psi = (\tau_1 \tau_3 \tau_2) \). Clearly, we then have a natural isomorphism \( \phi : S_3 \rightarrow \text{Aut}(S_3) \) by defining \( \phi(i) = \Xi, \phi(12) = \Delta, \phi(13) = \Lambda, \phi(23) = \Sigma, \phi(123) = \Phi, \) and \( \phi(132) = \Psi \). Thus, \( S_3 \equiv \text{Aut}(S_3) \).

We now will describe \( \text{Inn}(S_3) \). Since \( \text{Aut}(S_3) \equiv S_3 \) via our isomorphism \( \phi, \text{Aut}(S_3) = \langle \Delta, \Lambda, \Sigma \rangle, \) and so we first investigate \( \Delta, \Lambda, \) and \( \Sigma \). By direct computation, we note that \( \Delta(\tau) = i_{(23)}(\tau) \) for all transpositions \( \tau \in S_3 \), and hence \( \Delta(\rho) = \Delta(\prod_{i=1}^{m} \tau_i) = \prod_{i=1}^{m} \Delta(\tau_i) = \prod_{i=1}^{m} i_{(23)}(\tau_i) = i_{(23)}(\prod_{i=1}^{m} \tau_i) = i_{(23)}(\rho) \) for every \( \rho \in S_3 \), i.e. \( \Delta = i_{(23)} \). Note that \( (23) \) is the only transposition in \( S_3 \) that is fixed by \( \Delta \). By similar computations, we find \( \Lambda = i_{(13)} \) and \( \Sigma = i_{(12)} \). Thus, \( \Delta, \Lambda, \Sigma \in \text{Inn}(S_3) \). But then, since \( \text{Inn}(S_3) \) is a group under composition (and, in fact, since \( i_x \circ i_y = i_{xy} \) and using our isomorphism \( \phi : S_3 \rightarrow \text{Aut}(S_3) \), we have \( \Xi = \Delta^2 = i_{(23)(23)}^2 = i_{e} \in \text{Inn}(S_3), \Phi = \Lambda \circ \Delta = i_{(13)} \circ i_{(23)} = i_{(13)(23)} = i_{(13)} \in \text{Inn}(S_3), \) and \( \Psi = \Delta \circ \Lambda = i_{(23)} \circ i_{(13)} = i_{(23)(13)} = i_{(13)(23)} \in \text{Inn}(S_3) \). That is, we have shown that \( \text{Inn}(S_3) = \text{Aut}(S_3) / S_3, \) and hence \( \text{Out}(S_3) = \text{Aut}(S_3) / \text{Inn}(S_3) = S_3 / S_3 = \{ e \} \) is the trivial group. More generally, \( \text{Inn}(S_n) = \text{Aut}(S_n) / S_n \) for all natural numbers \( n \) except for \( n = 6 \).