James Lee Crowder

Math 430
Dr. Songhao Li
Spring 2016

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 $H \leq G$, 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 $H \leq G$, 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 $s \in S$, $(xy)(s) = x(ys) = x(sy) = (xs)y = (sx)y = s(xy)$, i.e. $xy \in C_G(S)$. Similarly, since $x \in C_G(S)$, $x^{-1}s = (x^{-1}s)\,e = (x^{-1}s)(xx^{-1}) = x^{-1}(sx)x^{-1} = x^{-1}(xs)x^{-1} = (x^{-1}x)(sx^{-1} = e\,(sx^{-1}) = sx^{-1}$, 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 $(xy)\,s = x\,(ys) = x\,(s'y) = (xs')\,y$ for some $s' \in S$. Similarly, since $xs' \in xS = Sx$, $(xs')\,y = (s''x)\,y = s''(xy) \in S(xy)$ 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

$x^{-1}s = (x^{-1}s)\,e = (x^{-1}s)(xx^{-1}) = x^{-1}(sx)x^{-1} = x^{-1}(xs')x^{-1} = (x^{-1}x)(s'x^{-1}) = e\,(s'x^{-1}) = s'x^{-1} \in Sx^{-1}$, 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 $H \leq G$. 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

$$\begin{aligned}(ncn^{-1})\,s &= (nc)(n^{-1}s)\\ &= (nc)(s'n^{-1})\\ &= n\,(cs')\,n^{-1}\\ &= n\,(s'c)\,n^{-1}\\ &= (ns')(cn^{-1})\\ &= (sn)(cn^{-1})\\ &= s\,(ncn^{-1})\end{aligned}$$

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, $C_G(S) \trianglelefteq N_G(S)$. ■

I will try and pick out the more interesting and/or challenging of the given recommended problems. If there is a problem you would like to know the solution to that is not shown here, try to make it to the recitation on Thursday. If you cannot make it, feel free to email me personally at james.crowder@wustl.edu and I will be able to at least write up a proof sketch for the problem in question.

Part III Section 13 Exercises

12. Show that $\phi : M_n(\mathbb{R}) \to \mathbb{R}$ defined by $\phi(A) = \det(A)$ is not a group homomorphism from the additive group of n by n matrices into $(\mathbb{R}, +)$ for $n \geq 2$.

Solution: If $n = 1$, then $M_n(\mathbb{R}) = \{[r] \;:\; r \in \mathbb{R}\}$, and so $\phi([r]) = \det([r]) = r$ does yield a group isomorphism: $\det([a] + [b]) = \det([a + b]) = a + b = \det([a]) + \det([b])$. Suppose $n \geq 2$. Then $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ are in $M_n(\mathbb{R})$ but $\det(A + B) = \det(I) = 1 \neq 0 + 0 = \det(A) + \det(B)$, and so ϕ is not a group homomorphism.

■

17. Let $\phi : \mathbb{Z} \to \mathbb{Z}_7$ be a group homomorphism with $\phi(1) = [4]$. Find $\ker\phi$ and $\phi(25)$.

Solution: Suppose $k \in \ker\phi$. Then $\phi(k) = [k] = [0]$. Then 7 divides $k = k - 0$, and so $k = 7m$ for some $m \in \mathbb{Z}$. Thus, $\ker\phi \subseteq 7\mathbb{Z}$. Conversely, if $7n \in 7\mathbb{Z}$, then $\phi(7n) = [7n] = [0]$ since 7 divides $7n = 7n - 0$. Thus, $\ker\phi = 7\mathbb{Z}$. Since ϕ is a group homomorphism, $\phi(25) = \phi(\sum_{i=1}^{25} 1) = \sum_{i=1}^{25} \phi(1) = \sum_{i=1}^{25} [4] = [100] = [2]$ since $100 - 2 = 98 = 7 \cdot 14$.

■

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

Proof. Clearly, since ϕ 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 $\Sigma : \phi[G] \to L_K$ by $\Sigma\big(\phi(g)\big) = gK$. We first show that Σ is well defined. Suppose $x \in G$ such that $\phi(x) = \phi(g)$. Then, since ϕ 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, $\Sigma\big(\phi(x)\big) = xK = gK = \Sigma\big(\phi(g)\big)$, and so Σ is well defined. This argument in reverse shows that Σ is injective. Since Σ is clearly surjective since $\phi(g) \in \phi[G]$ for all $gK \in L_K$, Σ is a bijection, as desired. Thus, $|\phi[G]| = |L_K| = (K : G)$, which divides $|G|$ by Lagrange's Theorem. ■

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

Proof. Since $\phi[G] \subseteq G'$, $|\phi[G]| \leq |G'|$, and so $|\phi[G]|$ is finite. By Theorem 13.12, $\phi[G] \leq G'$, and hence, by Lagrange's Theorem, $|\phi[G]|$ divides $|G'|$. ■

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

49. Show that if $\phi : G \to G'$ and $\psi : G' \to G''$ are group homomorphisms, then $\psi \circ \phi : G \to G''$ 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 ϕ is a group homomorphism, for any $x, y \in G$ we have

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

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

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

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

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:
$x \in \phi^{-1}[\phi(g)] \Leftrightarrow \phi(x) = \phi(g) \Leftrightarrow \phi(g^{-1}x) = e' \Leftrightarrow g^{-1}x \in K \Leftrightarrow x \in gK$. ∎

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

Proof.

($\Rightarrow$) Suppose ϕ is a group homomorphism. Then
$hk = \phi(1, 1) = \phi\big((0, 1) + (1, 0)\big) = \phi(0, 1)\,\phi(1, 0) = kh$.

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

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

i.e. ϕ 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 $i_x[H] = [K]$ 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 $N \trianglelefteq G$ 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_α 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, $\bigcap_{\alpha \in I} N_\alpha \trianglelefteq G$. ■

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

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 $\mathrm{Aut}(G)$. Since the identity map $\mathrm{id}_G : G \to$ defined by $\mathrm{id}_G(g) = g$ is clearly an automorphism, and isomorphisms are invertible, $\mathrm{Aut}(G)$ is a group under the usual function composition.

We now show that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. Since $i_e(g) = ege^{-1} = ege = g$ for all $g \in G$, $\mathrm{id}_G = i_e \in \mathrm{Inn}(G)$. Let $i_x, i_y \in \mathrm{Inn}(G)$. Then, for all $g \in G$,

$$i_x \circ i_y(g) = i_x\big(i_y(g)\big) = i_x(ygy^{-1}) = x(ygy^{-1})x^{-1} = (xy)g(y^{-1}x^{-1}) = (xy)g(xy)^{-1} = i_{xy}(g)$$

Thus, $i_x \circ i_y = i_{xy} \in \mathrm{Inn}(G)$. Similarly, $(i_x)^{-1} = i_{x^{-1}} \in \mathrm{Inn}(G)$ since

$$i_x \circ i_{x^{-1}}(g) = x(x^{-1}gx)x^{-1} = (xx^{-1})g(xx^{-1}) = ege = i_e(g) = ege = (x^{-1}x)g(x^{-1}x) = x^{-1}(xgx^{-1})x = i_{x^{-1}} \circ i_x(g)$$

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

$$\phi\, i_x\, \phi^{-1}(g) = \phi\Big(i_x\big(\phi^{-1}(g)\big)\Big) = \phi(x\phi^{-1}(g)x^{-1}) = \phi(x)\phi\big(\phi^{-1}(g)\big)\phi(x^{-1}) = \phi(x)\, g\, \phi(x)^{-1} = i_{\phi(x)}(g)$$

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

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 ϕ induces a group homomorphism $\phi_* : G/H \to G'/H'$.

Proof. Define ϕ_* by $\phi_*(gH) = \phi(g)H'$. We will first show that ϕ_* is well defined. Suppose $xH, yH \in G/H$ such that $\phi_*(xH) = \phi_*(yH)$. Then $\phi(x)H' = \phi(y)H'$. Then, since ϕ is a homomorphism and by definition of the group G'/H',

$$\phi(x^{-1}y)H' = \phi(x^{-1})\phi(y)H' = \phi(x)^{-1}\phi(y)H' = \phi(x)^{-1}H'\phi(y)H' = (\phi(x)H')^{-1}\phi(y)H' = H'$$

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, ϕ_* is well defined.

We now verify that ϕ_* is a group homomorphism. For any $aH, bH \in G/H$, since ϕ 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 $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$ by Problem 37, we can define the quotient group $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$. Describe $\mathrm{Out}(S_3)$.

Proof. We will first describe $\mathrm{Aut}(S_3)$. Since $S_3 = \langle (1\,2), (1\,3), (2\,3) \rangle$, $\Theta \in \mathrm{Aut}(S_3)$ is completely determined by $\Theta(1\,2), \Theta(1\,3)$, and $\Theta(2\,3)$. In order for Σ to be an automorphism of S_3, we must have $|\Theta(\lambda)| = |\lambda|$ for all $\lambda \in S_3$. In particular, Θ 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, Θ must map each transposition to a unique transposition. Thus, we have 6 candidate functions, one for each possible permutation of the transpositions $(1\,2), (1\,3)$, and $(2\,3)$, i.e. the functions $\Xi = \mathrm{id}_{S_3}$,
$\Delta(1\,2) = (1\,3),\ \Delta(1\,3) = (1\,2),\ \Delta(2\,3) = (2\,3),\quad \Lambda(1\,2) = (2\,3),\ \Lambda(1\,3) = (1\,3),\ \Lambda(2\,3) = (1\,2)$,
$\Sigma(1\,2) = (1\,2),\ \Sigma(1\,3) = (2\,3),\ \Sigma(2\,3) = (1\,3),\quad \Phi(1\,2) = (1\,2),\ \Phi(1\,3) = (2\,3),\ \Phi(2\,3) = (1\,2)$, and
$\Psi(1\,2) = (2\,3),\ \Psi(1\,3) = (1\,2),\ \Psi(2\,3) = (1\,3)$. 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 τ_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 Ψ is in fact an automorphism of S_3, and so $\mathrm{Aut}(S_3) = \{\Xi, \Delta, \Lambda, \Sigma, \Phi, \Psi\}$. Moreover, perhaps by labeling $(1\,2) = \tau_1$, $(1\,3) = \tau_2$, and $(2\,3) = \tau_3$, 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 $\phi : S_3 \to \mathrm{Aut}(S_3)$ by defining $\phi(\iota) = \Xi$, $\phi(1\,2) = \Delta$, $\phi(1\,3) = \Lambda$, $\phi(2\,3) = \Sigma$, $\phi(1\,2\,3) = \Phi$, and $\phi(1\,3\,2) = \Psi$. Thus, $S_3 \equiv \mathrm{Aut}(S_3)$.

We now will describe $\mathrm{Inn}(S_3)$. Since $\mathrm{Aut}(S_3) \equiv S_3$ via our isomorphism ϕ, $\mathrm{Aut}(S_3) = \langle \Delta, \Lambda, \Sigma \rangle$, and so we first investigate Δ, Λ, and Σ. By direct computation, we note that $\Delta(\tau) = i_{(2\,3)}(\tau)$ for all transpositions $\tau \in S_3$, and hence $\Delta(\rho) = \Delta(\prod_{i=1}^{m} \tau_i) = \prod_{i=1}^{m} \Delta(\tau_i) = \prod_{i=1}^{m} i_{(2\,3)}(\tau_i) = i_{(2\,3)}\left(\prod_{i=1}^{m} \tau_i\right) = i_{(2\,3)}(\rho)$ for every $\rho \in S_3$, i.e. $\Delta = i_{(2\,3)}$. Note that $(2\,3)$ is the only transposition in S_3 that is fixed by Δ. By similar computations, we find $\Lambda = i_{(1\,3)}$ and $\Sigma = i_{(1\,2)}$. Thus, $\Delta, \Lambda, \Sigma \in \mathrm{Inn}(S_3)$. But then, since $\mathrm{Inn}(S_3)$ is a group under composition (and, in fact, since $i_x \circ i_y = i_{xy}$) and using our isomorphism $\phi : S_3 \to \mathrm{Aut}(S_3)$, we have $\Xi = \Delta^2 = i_{(2,3)}^2 = i_{(2\,3)^2} = i_e \in \mathrm{Inn}(S_3)$, $\Phi = \Lambda \circ \Delta = i_{(1\,3)} \circ i_{(2\,3)} = i_{(1\,3)(2\,3)} = i_{(1\,3\,2)} \in \mathrm{Inn}(S_3)$, and $\Psi = \Delta \circ \Lambda = i_{(2\,3)} \circ i_{(1\,3)} = i_{(2\,3)(1\,3)} = i_{(1\,2\,3)} \in \mathrm{Inn}(S_3)$. That is, we have shown that $\mathrm{Inn}(S_3) = \mathrm{Aut}(S_3) \equiv S_3$, and hence $\mathrm{Out}(S_3) = \mathrm{Aut}(S_3)/\mathrm{Inn}(S_3) = S_3/S_3 \equiv \{e\}$ is the trivial group. More generally, $\mathrm{Inn}(S_n) = \mathrm{Aut}(S_n) \equiv S_n$ for all natural numbers n except for $n = 6$. ■