Spring 2024: Math 791 Exam 1 Solutions

For this exam, you may use your notes, the Daily Summary, and any homework (giving complete details), but you may not consult **any other sources**, including: any algebra textbook, the internet, classmates or any other students not in this class, or any professor except your Math 791 instructor. You may not cite any group theoretical facts not covered in class or the homework. To receive full credit, all proofs must be complete and contain the appropriate amount of detail. Please upload a pdf copy of your solutions to Canvas no later than 6pm on Monday, February 19.

Good luck on the exam!

1. Treating $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ as abelian groups under addition, consider the abelian group $\mathbb{Q}/\mathbb{Z}$. Prove:
   (i) Every element of $\mathbb{Q}/\mathbb{Z}$ is a coset of the form $q+\mathbb{Z}$, with $0 \leq q < 1$.
   (ii) Every element of $\mathbb{Q}/\mathbb{Z}$ has finite order, but there are elements in $\mathbb{Q}/\mathbb{Z}$ of arbitrarily large order.
   (iii) $\mathbb{Q}/\mathbb{Z}$ is the subgroup of $\mathbb{R}/\mathbb{Z}$ of elements of finite order.

Solution. For (i), suppose $r+\mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. We may write $r = r_0 + n$, where n is an integer and $0 \leq r_0 < 1$. But then $r+\mathbb{Z} = (r_0+n)+\mathbb{Z} = r_0+\mathbb{Z}$.

For (ii), if $r+\mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$, write $r = \frac{a}{b}$, with $a, b \in \mathbb{Z}$, and $b > 0$. Then $b \cdot r$, which is r added to itself b times, equals a as an element of $\mathbb{Z}$. This shows that in $\mathbb{Q}/\mathbb{Z}$, $r+\mathbb{Z}$ added to itself finitely many times is $a+\mathbb{Z} = 0+\mathbb{Z}$. Thus, $r+\mathbb{Z}$ has finite order. For $n \geq 1$, $\frac{1}{n}+\mathbb{Z}$ clearly has order n, so that $\mathbb{Q}/\mathbb{Z}$ has elements of arbitrarily large order.

For (iii), let $\rho+\mathbb{Z} \in \mathbb{R}/\mathbb{Z}$ have finite order, for $\rho \in \mathbb{R}$. Then $n(\rho+\mathbb{Z}) = n\rho+\mathbb{Z} = 0+\mathbb{Z}$, for some integer $n \geq 1$. Thus, $n\rho \in \mathbb{Z}$, so that $n\rho = m$, for some $m \in \mathbb{Z}$. But this implies $\rho \in \mathbb{Q}$, and therefore, $\mathbb{Q}/\mathbb{Z}$ is the set of elements of finite order in $\mathbb{R}/\mathbb{Z}$. □

2. Let H be subgroup of the group G and suppose $\{g_\alpha H\}_{\alpha \in A}$ are the distinct left cosets of H in G. Prove that H is normal in G if for all $\alpha \in A$, $g_\alpha H = Hg_\alpha$.

Solution. Let $g \in G$. Then $g \in g_\alpha H$, for some α. Thus, $g \in gH = g_\alpha H = Hg_\rho$, which implies $Hg = Hg_\rho$. Thus, $gH = Hg$, which shows that H is normal in G. □

3. Let H, K be subgroups of G.
   (i) Show that HK is a subgroup of G if and only if $HK = KH$. Conclude that if K is normal in G, then HK is a subgroup.
   (ii) Suppose H, K are finite. Show that $|HK| \cdot |H \cap K| = |H| \cdot |K|$. Here we do not assume that HK is a subgroup of G.

Solution. For part (i), suppose $HK = KH$. Take $hk \in HK$. Then $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. Suppose $hk, h_1k_1 \in HK$. Then, $(hk)(h_1k_1) = h(kh_1)k_1 = hh'k'k_1 \in HK$, since $kh_1 \in KH = HK$. Thus HK is a subgroup. Conversely, suppose HK is a subgroup. Let $kh \in KH$. Then $kh = (h^{-1}k^{-1})^{-1} \in HK$, thus $KH \subseteq HK$. Now suppose $h \in H, k \in K$. Then $(ek^{-1})(h^{-1}e)$ is a product of elements in HK, so $(ek^{-1})(h^{-1}e) = h_1k_1$, for $h_1k_1 \in HK$, since HK is a subgroup. Taking inverses, we have $hk = k_1^{-1}h_1^{-1} \in KH$, showing $HK \subseteq KH$, which gives what we want.

For (ii), we use the following observation. Suppose $f : X \to Y$ is a surjective set function between finite sets X and Y such that for all $y \in Y$, $|f^{-1}(y)| = r$. Then $|Y| \cdot r = |X|$. This follows since X is the disjoint union of the sets $f^{-1}(y)$, as y ranges over the elements in X. With this in mind, set $r := |H \cap K|$ and let $f : H \times K \to HK$ be the set function taking each (h, k) in $H \times K$ to hk in HK. We need to show that each $hk \in HK$ has r pre-images in $H \times K$. Fix $hk \in HK$. For each $x \in H \cap K$, we have r distinct elements $(hx, x^{-1}k)$ such that $f(hx, x^{-1}k) = hk$. Suppose $f(h_1, k_1) = hk$, i.e., $h_1k_1 = hk$. Then $h^{-1}h_1 = kk_1^{-1}$. Calling this element y, we have $y \in H \cap K$. Thus, $h_1 = hy$ and $k_1 = y^{-1}k$, showing that we have accounted for all of the elements in $f^{-1}(hk)$. Thus, $|f^{-1}(hk)| = r$. □

4. Let G be a group and $H \subseteq G$ a proper subgroup. The *normalizer* of H in G is the set $N_G(H) := \{g \in G \mid gHg^{-1} = H\}$.
   (i) Show that $N_G(H)$ is the largest subgroup of G in which H is normal
   (ii) Show that there is a 1-1 correspondence between the distinct (left) cosets of $N_G(H)$ and the distinct conjugates of H.
   (iii) Show that if G is finite, then $G \neq \bigcup_{g \in G} gHg^{-1}$.
   (iv) Let $G = \mathrm{Gl}_2(\mathbb{C})$ and H be the subgroup of lower triangular matrices. Show that $G = \bigcup_{g \in G} gHg^{-1}$. Hint: Use the Jordan Canonical Form theorem.

Solution. For (i), suppose $a, b \in N_G(H)$. Then $abH(ab)^{-1} = abHb^{-1}a^{-1} = aHa^{-1} = H$, so $ab, \in N_G(H)$. Suppose $a^{-1}ha \in a^{-1}Ha$. Then, $h = ah'a^{-1}$, for some $h' \in H$. Thus, $a^{-1}ha = a^{-1}(ah'a^{-1})a = h' \in H$, showing $a^{-1}Ha \subseteq H$. The reverse containment is similar. Thus, $a^{-1}Ha = H$, so $N_G(H)$ is a subgroup. Suppose K is a subgroup of G containing H in which H is normal. Then $kHk^{-1} = H$, for all $k \in K$, so that $K \subseteq N_G(H)$, showing that $N_G(H)$ is the largest subgroup of G in which H is normal.

For (ii), if now X denotes the set of distinct conjugates of H and Y denotes the set of distinct left cosets of $N_G(H)$, we define $\phi : X \to Y$ by $\phi(gHg^{-1}) = gN_G(H)$. Then $aHa^{-1} = bHb^{-1}$ if and only if $(b^{-1}a)Ha^{-1}b = H$ if and only if $(b^{-1}a)H(b^{-1}a)^{-1} = H$ if and only if $b^{-1}a \in N_G(H)$ if and only if $aN_G(H) = bN_G(H)$, showing that ϕ is well-defined and 1-1. Moreover, ψ is clearly onto, which gives what we want.

For (iii), by (ii), if $g_1Hg_1^{-1}, \ldots, g_rHg_r^{-1}$ are the distinct conjugates of H, then $g_1N_G(H), \ldots, g_rN_G(H)$ are the distinct left cosets of $N_G(H)$. Now, G is the disjoint union of the cosets $g_iN_G(H)$, so that $|G| = r \cdot |N_G(H)|$. On the other hand, $|g_iHg_i^{-1}| = |H| \leq |N_G(H)|$ and $|\bigcup_i g_iHg_i^{-1}| < r \cdot |H|$, since e belongs to each $g_iHg_i^{-1}$. Thus, we cannot have $G = \bigcup_i g_iHg_i^{-1}$.

For (iv), if $A \in G$, then there exists $g \in G$ such that $g^{-1}Ag$ is in JCF, which is lower triangular. Note, that since A is invertible, its eigenvalues are non-zero, so that $g^{-1}Ag \in G$, and therefore $g^{-1}Ag \in H$. Thus, $A \in gHg^{-1}$, which gives what we want. □

5. Prove the following facts about the group S_n.
   (i) The conjugacy class of any single k-cycle is the set of all k-cycles.
   (ii) For $\tau := (1, 2, \ldots, n)$, the centralizer of τ in S_n is just $\langle\tau\rangle$. Hint: Consider the conjugacy class of τ.

Solution. For (i) we first fix $\tau = (i_1, \ldots, i_k)$ a k-cycle, and take any $\gamma \in S_n$. We note that $\gamma\tau\gamma^{-1} = (\gamma(i_1), \ldots, \gamma(i_k))$, since $\gamma\tau\gamma^{-1}(\gamma(i_j)) = \gamma(i_{j+1})$, for $1 \leq j \leq k-1$ and $\gamma\tau\gamma^{-1}(\gamma(i_k)) = \gamma(i_1)$. If $j \notin \{\gamma(i_1), \ldots, \gamma(i_k)\}$, then $\gamma^{-1}(j) \notin \{i_1, \ldots, i_k\}$, so that $\gamma\tau\gamma^{-1}(j) = \gamma\gamma^{-1}(j) = j$, which gives what we want. This shows that conjugacy class of τ is contained in the set of all k-cycles. On the other hand if $\sigma := (j_1, \ldots, j_k)$ is an arbitrary k-cycle and we define γ as follows: $\gamma(i_1) = j_1, \ldots, \tau(i_k) = j_k$, and $\gamma(s) = s$, for $s \notin \{i_1, \ldots, i_k\}$, then by what we have just shown, $\gamma\tau\gamma^{-1} = \sigma$. Thus, any k-cycle is in the conjugacy class of τ, which gives what we want.

For (ii), by part (i), the conjugacy class of τ is the set of all n-cycles. Since there are $(n-1)!$ n-cycles (check this!), the conjugacy class of τ has $(n-1)!$ elements. Thus, $[S_n : C_{S_n}(\tau)] = (n-1)!$. Therefore $|C_{S_n}(\tau)| = n$. Since $o(\tau) = n$ and $\tau \in C_{S_n}(\tau)$, this forces $\langle\tau\rangle = C_{S_n}(\tau)$, which is what we want. □

6. For the symmetric group S_n show that: (i) That the center of S_n is $\{id\}$, for $n \geq 3$ and (ii) $S_n = \langle(1, 2), (1, 2, \ldots, n)\rangle$.

Solution. For (i), let $\sigma \in S_n$ be a non-identity element. Then $\sigma(i) = j$, for some $i \neq j \in X := \{1, 2, \ldots, n\}$. Take $k \in X\backslash\{i, j\}$, and let τ be any element in S_n satisfying $\tau(i) = i$ and $\tau(j) = k$. Then, $\sigma\tau(i) = \sigma(i) = j$ and $\tau\sigma(i) = \tau(j) = k$, showing that $\sigma\tau \neq \tau\sigma$. Thus, given any non-identity element $\sigma \in S_n$ $\sigma \notin Z(S_n)$, so $Z(S_n) = \{id\}$.

For (ii), set $\sigma := (1, 2)$ and $\tau := (1, 2, \ldots, n)$. Problem 5 shows that for any 2-cycle (a, b) and $\gamma \in S_n$, $\gamma(a, b)\gamma^{-1} = (\gamma(a), \gamma(b))$. Thus, since $\tau^{i-1}(1) = i$ and $\tau^{i-1}(2) = i+1$, it follows that $\tau^{i-1}(1, 2)\tau^{-(i-1)} = (i, i+1)$ belongs to the subgroup generated by σ and τ. Since S_n is generated by 2-cycles, it suffices to show that any 2-cycle is a product of 2-cycles with adjacent entries. Let (a, b) be a 2-cycle, and we assume $a < b$. Say , $b = a + i$, with $i \geq 1$. Then,

$$(a, b) = (a, a+1)(a+1, a+2)\cdots(a+i-2, a+i-1)(a+i-1, b)(a+i-2, a+i-1)\cdots(a+1, a+2)(a, a+1). \quad \square$$

7. Prove the statements below to establish the following fact: For $n \geq 5$, A_n is the only non-trivial normal subgroup of S_n.
   (i) Let G be a group and A, B normal subgroups of G. Show that $A \cap B$ is a normal subgroup. Conclude that if A is a simple group, then $A \cap B = \{e\}$.
   (ii) Suppose G is a group and $A \subseteq G$ is a normal subgroup of index two. Let $B \subseteq G$ be a normal subgroup. Show that if A is a simple group, then B must have order two. (Hint: For $b_1, b_2 \in B$, consider the cosets b_1A and b_2A.)
   (iii) Let G be a group and $B = \{e, b\}$ a normal subgroup of order two. Then $b \in Z(G)$, the center of G.
   (iv) Suppose G is a group, and $A \subseteq G$ is a normal subgroup of index two. Show that if A is a simple group and $Z(G) = \{e\}$, then A is the only proper normal subgroup of G.

Conclude that A_n is the only proper normal subgroup of S_n, for $n \geq 5$.

Solution. (i) This is pretty clear. $A \cap B$ is easily seen to be a subgroup, and if $x \in A \cap B$ and $g \in G$, then $gxg^{-1} \in A$ and $gxg^{-1} \in B$, so $gxg^{-1} \in A \cap B$, showing that $A \cap B$ is normal in G. Since $A \cap B$ is also normal in A, if A is simple then $A \cap B = \{e\}$.

(ii) To see this, first note that by (i) $A \cap B = \{e\}$. Now, suppose $b_1, b_2 \in B$ are non-identity elements. Then $b_1, b_2 \notin A$, and thus $b_1A = b_2A$, since A has index two. Therefore, $b_2^{-1}b_1 \in A$ and thus $b_2^{-1}b_2 \in A \cap B = e$, so that $b_1 = b_2$. Thus, B has two elements.

(iii) This follows, since, for all $g \in g$, $g^{-1}bg = b$, so $bg = gb$, i.e., $b \in Z(G)$.

(iv) This follows from the previous step, since if there there were another normal subgroup, it would have to be contained in $Z(G)$.

So now, to apply the above to S_n with, $n \geq 5$: A_n is a simple group of index two. To see that A_n is the only normal subgroup of S_n it suffices by (iv) to see that $Z(S_n) = \{e\}$. But this follows from problem 6 □.

8. Let G be a non-abelian group of order p^3, p a prime. How many conjugacy classes with more than one element does G have?

Solution. By the class equation, $Z(G)$, the center of G is not trivial. Since G is non-abelian, $|Z(G)| = p$ or p^2. If $|Z(G)| = p^2$, $G/Z(G)$ has order p, so that $G/Z(G)$ is cyclic. Since this implies G is abelian, we must have $|Z(G)| = p$. Thus, the class equation becomes:

$$\begin{aligned} p^3 = |G| &= p + \Sigma_{i=1}^r |c(x_i)| \\ &= p + \Sigma_{i=1}^r [G : C_G(x_i)], \end{aligned}$$

where the sum is taken over the conjugacy classes with more than one element. If for some $1 \leq i \leq r$, $[G : C_G(x_i)] = p^2$, $C_G(x_i)| = p$ and it would then follow that $Z(G) = C_G(x_i)$, which is a contradiction, since $x_i \notin Z(G)$. Thus, we have that $[G : C_G(x_i)] = p$. Therefore, $p^3 = p + rp$, which implies $r = p^2 - 1$. $\square$

9. Recall that if G acts on a set X with n elements, there exists a group homomorphism $\phi : G \to S_n$.
   (i) Find an *explicit* group homomorphism from $\mathbb{Z}_2 \times \mathbb{Z}_2 \to S_4$.
   (ii) Let Q_8 act on itself via left multiplication. Use this action to find an explicit group homomorphism from Q_8 to S_8. Now find two elements in S_8 that generate a subgroup isomorphic to Q_8.

You may use the theorem from class to infer that the maps into S_4 and S_8 you construct are group homomorphisms.

Solution. For (i), label the elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$ as follows: $g_1 := (0,0), g_2 := (1,0), g_3 := (0,1), g_4 := (1,1)$. We define $\phi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to S_4$ as follows: $\phi(0,0) = id$. To see what $\phi(g_2)$ should be, we let g_2 act on $\mathbb{Z}_2 \times \mathbb{Z}_2$ via the group operation $g_2 + g_1 = g_2, g_2 + g_2 = g_1, g_2 + g_3 = g_4, g_2 + g_4 = g_3$, so we define $\phi(g_2) := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$. Similarly, if we let g_3, g_4 act on $\mathbb{Z}_2 \times \mathbb{Z}_2$, we se $\phi(g_3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ and $\phi(g_4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$. It is straight forward now to check that ϕ is a group homomorphism, e.g.,

$$\phi(g_2 + g_3) = \phi(g_4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \phi(g_2)\phi(g_3).$$

Part (ii) is similar to part (i). If we label the elements in Q_8 as $g_1 = 1, g_2 = -1, g_3 = i, g_4 = -i, g_5 = j, g_6 = -j, g_7 = k, g_8 = -k$, and we let each element act on Q_8 via multiplication, we will get $\phi : Q_8 \to S_8$ satisfying $\phi(1) = id$, $\phi(-1) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \end{pmatrix}$, $\phi(i) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 2 & 1 & 7 & 8 & 6 & 5 \end{pmatrix}$, $\phi(j) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 8 & 7 & 2 & 1 & 3 & 4 \end{pmatrix}$, etc. Since $Q_8 = \langle i, j \rangle$, it follows that $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 2 & 1 & 7 & 8 & 6 & 5 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 8 & 7 & 2 & 1 & 3 & 4 \end{pmatrix}$ generate a subgroup of S_8 isomorphic to Q_8. $\square$

10. Show that A_4 does not have a subgroup of order six. This shows that the converse of Lagrange's theorem does not hold. (Hint: Use Cauchy's theorem).

Solution. Suppose $H \subseteq A_4$ is a subgroup of order six. Since $|A_4| = 12$, H has index two and thus is normal in A_4. On the other hand, by Cauchy's Theorem, H has an element of order two, say σ and an element of order three, say τ, which is necessarily a 3-cycle. By re-indexing X_4, without loss of generality, we may assume $\tau = (1,2,3)$. Thus, H contains the elements, $e, \sigma, \tau, \tau^2 = (1,3,2)$. Consider the 3-cycle $(2,3,4) \in A_4$. Then

$$(2,3,4)(1,2,3)(2,3,4)^{-1} = (2,3,4)(1,2,3)(2,4,3) = (1,3,4) \in H.$$

Therefore $(1,3,4)^2 = (1,4,3)$ also belongs to H. Counting the identity element, we now have six elements in H. But $(2,4,3)(1,2,3)(2,3,4) = (1,4,2)$ belongs to H, which gives seven distinct elements in H, which is a contradiction. Thus, there are no subgroups of order six in A_4.

In fact, one can show that the subgroups of A_4 are:
   (i) The three subgroups of order two: $\{e, (1,2)(3,4)\}, \{e, (1,3)(2,4)\}, \{e, (1,4)(2,3)\}$
   (ii) The four subgroups of order three having the form $\{e, (i_1, i_2, i_3), (i_1, i_3, i_2)\}$
   (iii) The one subgroup of order four: $\{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. $\square$

Bonus Problems. Bonus problems must be essentially fully correct to receive any credit.

BP 1. Let $\sigma \in S_n$ and write $\sigma = \tau_1 \cdots \tau_r$, a product of disjoint cycles. Suppose each τ_i is a k_i-cycle. The *cycle type* of σ is the set $\{k_1, \ldots, k_r\}$. Prove that two elements in S_n are conjugate if and only if they have the same cycle type. Thus, the conjugacy classes in S_n are determined by cycle type.

Solution. By problem five, for any k-cycle σ, its conjugacy class is the set of all k-cycles, and hence is the set of all permutations with the same cycle type.

Now, if $\sigma \in S_n$ is written as a product of disjoint cycles $\tau_1 \cdots \tau_r$, where τ_i is a k_i-cycle, then by problem five, for any $\gamma \in S_n$, $\gamma\sigma\gamma^{-1} = (\gamma\tau_1\gamma^{-1})(\gamma\tau_2\gamma^{-1}) \cdots (\gamma\tau_r\gamma^{-1})$, which is a product of disjoint cycles of type $k_1, \ldots, k_r$. Thus, if two elements of S_n are conjugate, they have the same cycle type.

Now suppose $\tau_1 \cdots \tau_r$ and $\sigma_1 \cdots \sigma_r$ have cycle type $\{k_1, \ldots, k_r\}$. For each $1 \leq c \leq r$, we write $\tau_c = (i_{c1}, \ldots, i_{ck_c})$ and $\sigma_c = (j_{c1}, \ldots, j_{ck_c})$. We now define $\gamma(i_{c1}) = j_{c1}, \ldots, \gamma(i_{ck_c}) = j_{ck_c}$, for all $1 \leq c \leq r$, and $\gamma(s) = s$, for any $S \notin \{i_{cd}\}_{1 \leq c \leq r, 1 \leq d \leq k_c}$. Note that since the cycles τ_c are disjoint, γ is well-defined. By what we have shown in the case of one cycle, we have $\gamma\tau_c\gamma^{-1} = \sigma_c$, for all $1 \leq c \leq r$. Thus,

$$\gamma\tau_1\tau_2 \cdots \tau_r\gamma^{-1} = \gamma\tau_1\gamma^{-1}\gamma\tau_2\gamma^{-1} \cdots \gamma\tau_r\gamma^{-1} = \sigma_1\sigma_2 \cdots \sigma_r,$$

which shows that any two permutations with the same cycle type are conjugate. Thus, the conjugacy class of any permutation equals the set of all permutations having the same cycle type. $\square$

BP 2. Let $\sigma \in A_n$ and write $c(\sigma)$ for the conjugacy class of σ in S_n. Show that either $c(\sigma)$ is a conjugacy class in A_n or $c(\sigma)$ is the disjoint union of two conjugacy classes in A_n of equal order.

Solution. Let $c_{A_n}(\sigma)$ denote the conjugacy class of σ in A_n. We have $|c(\sigma)| = [S_n : C_{S_n}(\sigma)]$. Suppose $C_{S_n}(\sigma) \subseteq A_n$. Then

$$|c(\sigma)| = [S_n : C_{S_n}(\sigma)] = [S_n : A_n] \cdot [A_n : C_{S_n}(\sigma)] = 2 \cdot [A_n : C_{S_n}(\sigma)] = 2 \cdot |c_{A_n}(\sigma)|.$$

Set $r := [A_n : C_{S_n}(\sigma)]$ and let $a_1C_{S_n}(\sigma), \ldots, a_rC_{S_n}(\sigma)$ denote the distinct left cosets of $C_{S_n}(\sigma)$ in A_n (say $a_1 = e$). Then they are also distinct left cosets of $C_{S_n}(\sigma)$ in S_n. It follows that there exist $\gamma_1, \ldots, \gamma_r \in S_n \backslash A_n$ such that

$$a_1C_{S_n}(\sigma), \ldots, a_rC_{S_n}(\sigma), \gamma_1C_{S_n}(\sigma), \ldots, \gamma_rC_{S_n}(\sigma)$$

are the distinct left cosets of $C_{S_n}(\sigma)$ in S_n. Thus,

$$c(\sigma) = \{a_1\sigma a_1^{-1}, \ldots, a_r\sigma a_r^{-1}\} \cup \{\gamma_1\sigma\gamma_1^{-1}, \ldots, \gamma_r\sigma\gamma_r^{-1}\}, \qquad (**)$$

a disjoint union. Since each γ_i is an odd permutation, we may write $\gamma_i = b_i(1,2)$, where $b_i \in A_n$. Thus, each $\gamma_i\sigma\gamma_i^{-1} = b_i((1,2)\sigma(1,2))b_i^{-1}$ showing that each $\gamma_i\sigma\gamma_i^{-1}$ is an A_n conjugate of $(1,2)\sigma(1,2) \in A_n$. Since the group $(1,2)C_{S_n}(\sigma)(1,2)$ is contained in A_n and is isomorphic to $C_{S_n}(\sigma)$, the number of A_n conjugates of $(1,2)\sigma(1,2)$ equals the number of A_n conjugates of σ. Thus (**) shows that $c(\sigma)$ is the disjoint union of two conjugacy class in A_n having the same number of elements.

Now suppose $C_{S_n}(\sigma) \nsubseteq A_n$. We will show $c_{A_n}(\sigma) = c(\sigma)$. Clearly, $c_{A_n}(\sigma) \subseteq c(\sigma)$. Let $g\sigma g^{-1} \in c(\sigma)$. If g is even, then $g\sigma g^{-1} \in c_{A_n}(\sigma)$. Suppose g is odd. Let $\tau \in C_{S_n}(\sigma)$ be an odd permutation, which exists by assumption. Then $g\tau$ is even, and we have, $(g\tau)\sigma(g\tau)^{-1} = g\tau\sigma\tau^{-1}g^{-1} = g\sigma g^{-1}$ showing that $g\sigma g^{-1} \in c_{A_n}(\sigma)$. Thus, $c(\sigma) = c_{A_n}(\sigma)$, as required. □

BP3. Use Sylow theory to show that a group of order 144 is not a simple group. Hint: At some point, you should consider the centralizer of an element of order 3.

Solution. Write $|G| = 144 = 2^4 \cdot 3^2$. The possible number of Sylow 3-subgroups is: 1, 4, 16. If there is one, Sylow 3-subgroups, it is normal. If there are four Sylow 3-subgroups, then G acting on the set of Sylow 3-subgroups gives rise to a group homomorphism $\phi : G \to S_4$, which must have non-trivial kernel, and hence G has a normal subgroup. Now suppose G has 16 Sylow 3-subgroups. If pair-wise they all intersect in (e), then G has $16 \cdot 8 = 128$ elements of order 3 or 9. There are then just 16 remaining elements in G, which leaves room for just one Sylow 2-subgroup, which is then normal in G.

Suppose P_1, P_2 are Sylow 3-subgroups and $P_1 \cap P_2 \neq (e)$. Then $|P_1 \cap P_2| = 3$, so that $P_1 \cap P_2 = \langle x \rangle$ for x an element x of order 3. Since P_1, P_2 have order 9, they are abelian. Thus, $P_1, P_2 \subseteq C_G(x)$, which implies $P_1P_2 \subseteq C_G(x)$. Thus: $|C_G(x)| \geq |P_1P_2| = 27$, $|C_G(x)|$ is divisible by 9 (since $P_1 \subseteq C_G(x)$), and $|C_G(x)|$ divides 144. This gives $|C_G(x)| = 72$ or 36. In the first case, $C_G(x)$ has index 2, and is thus normal in G. In the second case, $C_G(x)$ has index 4, which yields a group homomorphism from G to S_4, which must have non-trivial kernel. Thus, in all cases, G contains a non-trivial normal subgroup.