SPRING 2023: MATH 791 EXAM 1 SOLUTIONS

For this exam, you may use your notes, the Daily Summary, and any homework you have done, but you may not consult any other sources, including, any algebra textbook, the internet, graduate 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 5pm on Monday, February 20.

Good luck on the exam!

1. Let G be a group and $H \subseteq G$ a proper subgroup. The *normalizer* of H 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 and there is a 1-1 correspondence between the distinct (left) cosets of $N_G(H)$ and the distinct conjugates of H. (2 points)
   (ii) Show that if G is finite, then $G \neq \bigcup_{g\in G} gHg^{-1}$. (5 points)
   (iii) Let $G = \mathrm{Gl}_2(\mathbb{C})$ and H be the subgroup of invertible lower triangular matrices. Show that $G = \bigcup_{g\in G} gHg^{-1}$. Hint: Use the Jordan Canonical Form theorem. (3 points)

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.

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 (ii), by (i), 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 (iii), 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. □

2. Let $\sigma \in S_n$, and write $\sigma = \tau_1\tau_2\cdots\tau_r$ as a product of disjoint cycles. Suppose τ_i is a k_i-cycle. We say that the *cycle type* of σ is $\{k_1, \ldots, k_r\}$, which is an unordered list, as disjoint cycles commute.
   (i) Prove that any two permutations are conjugate if and only if they have the same cycle type. Hint: First consider the case of a cycle. (5 points)
   (ii) Show that 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. (5 points)

Solution. For (i), first consider the case of a k-cycle. Let $\tau = (i_1, \ldots, i_k)$ be a k-cycle, and $\gamma \in S_n$. It follows that $\gamma\tau\gamma^{-1} = (\gamma(i_1), \ldots, \gamma(i_k))$. To see this, note that $\gamma\tau\gamma^{-1}(\gamma(i_j)) = \gamma(i_{j+1})$, 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 a 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.

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 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 $1 \leq c \leq r$, 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.

For (ii), by what we have just shown, 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. □

3. Recalling that if G acts on a set X with n elements, there exists a group homomorphism $\phi : G \to S_n$.
   (i) Prove that if $\phi : G \to S_n$ is a group homomorphism, then G acts on the set $X = \{x_1, \ldots, x_n\}$. (4 points)
   (ii) Find an *explicit* group homomorphism from $\mathbb{Z}_2 \times \mathbb{Z}_2 \to S_4$. (3 points)
   (iii) 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. (3 points)

Solution. For (i), define $g \cdot x_i := x_{\phi(g)(i)}$, for all $g \in G$ and $x_i \in X$. Then, $e \cdot x_i = x_{\phi(e)(i)} = x_i$, for all $x_i \in X$, since $\phi(e) \in S_n$ is the identity permutation. Moreover, if $a, b \in G$,

$$ab \cdot x_i = x_{\phi(ab)(i)} = x_{\phi(a)(\phi(b)(i))} = a \cdot x_{\phi(b)(i)} = a \cdot (b \cdot x_i),$$

so that ϕ induces an action of G on X.

For (ii), number 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 (iii) is similar to part (ii). If we number 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. □

4. Let G be a group satisfying $|G| = p^2$, where p is a prime. Show that G is isomorphic to $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$. (10 points)

Solution. We first show that G is abelian. As shown in class, the class equation gives that $Z(G) \neq \{e\}$. Since $|Z(G)|$ divides p^2, we have $|Z(G)| = p^2$ or p. In the first case, $G = Z(G)$, so G is abelian. In the second case, $G/Z(G)$ has order p and is therefore cyclic. From Homework 4 this implies G is abelian. To see this, assume $G/Z(G) = \langle gZ(G)\rangle$, and take $a, b \in G$. Then $a \in g^iZ(G)$ and $b \in g^jZ(G)$, for some i, j. Thus, $a = g^iz_1$ and $b = g^jz_2$, for some $z_1, z_2 \in Z(G)$. Thus,

$$\begin{aligned} ab &= (g^iz_1)(g^j(z_2) \\ &= g^{i+j}z_2z_2 \\ &= g^jz_2g^iz_2 \\ &= ba, \end{aligned}$$

which is what we want. Now, if G has an element of order p^2, then G is cyclic, and therefore isomorphic to $\mathbb{Z}_{p^2}$. Otherwise, evey non-identity element of G has order p. Take $e \neq a \in G$ and $b \notin \langle a\rangle$. We claim that the elements a^ib^j such that $0 \leq i, j \leq p-1$ are distinct. Suppose $a^ib^j = a^rb^s$, with $0 \leq i, j, r, s \leq p-1$. Then $a^{-r+i} = b^{s-j}$, and this element belongs to $\langle a\rangle \cap \langle b\rangle$. However, $\langle a\rangle \cap \langle b\rangle$ is a subgroup of $\langle a\rangle$, which has order p. By Lagrange's theorem, this forces $\langle a\rangle \cap \langle b\rangle$ to either have one element, or be equal to $\langle a\rangle$. Since $b \notin \langle a\rangle$, we must have $\langle a\rangle \cap \langle b\rangle = \{e\}$. Thus, $a^{-r+i} = e$ and $b^{s-j} = e$. Therefore, $a^i = a^r$ and $b^j = b^s$. Since $0 \leq i, j, r, s \leq p-1$, this forces $i = r, j = s$, so the

elements $\{a^i b^j\}$, with $0 \leq i, j \leq p-1$ are distinct. Since there are p^2 such elements, these are precisely the elements of G.

We now define $\phi : G \to \mathbb{Z}_p \times \mathbb{Z}_p$ by $\phi(a^i b^j) = (\overline{i}, \overline{j})$. Note that ϕ is well-defined, since the expressions $a^i b^j$, with $0 \leq i, j \leq p-1$ are unique. Now consider $a^i b^j, a^r b^s \in G$. Write $i + r = pq + u$ and $j + s = ph + v$, where $0 \leq v, h < p$. Note, it could be that q or h (or both) are zero. Using that $a^p = b^p = e$, we have,

$$\begin{aligned}
\phi(a^i b^j \cdot a^r b^s) &= \phi(a^{i+r} b^{j+s}) \\
&= \phi(a^u b^v) \\
&= (\overline{u}, \overline{v}) \\
&= (\overline{i+r}, \overline{j+s}) \\
&= (\overline{i}, \overline{j}) + (\overline{r}, \overline{s}) \\
&= \phi(a^i b^j) + \phi(a^r b^s),
\end{aligned}$$

showing that ϕ is a group homomorphism. It is clear that ϕ is surjective. Finally, if $\phi(a^i b^j) = (\overline{0}, \overline{0})$, then $\overline{i} \equiv 0 \bmod p$ and $\overline{j} \equiv 0 \bmod p$. Since $0 \leq i, j \leq p-1$, we have $i = 0 = j$, and thus $a^i b^j = e$, showing that ϕ is injective. Thus, $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$. □

5. Let H, K be groups admitting a group homomorphism $\phi : K \to \mathrm{Aut}(H)$, where $\mathrm{Aut}(H)$ denotes the automorphism group of H. This problem constructs the *semi-direct product* of H and K, denoted $H \rtimes_\phi K$.

(i) Show that K acts on H via ϕ, i.e., $k \cdot h := \phi(k)(h)$ defines an action of K on H. (2 points)
(ii) Define a binary operation on $H \rtimes_\phi K$ as follows: $(h_1, k_1)(h_2, k_2) := (h_1(k_1 \cdot h_2), k_1 k_2)$. Show that $H \rtimes_\phi K$ is a group under this binary operation. (2 points)
(iii) Show that H and K are isomorphic to their natural images $H' := \{(h, 1) \mid h \in H\}$, and $K' := \{(1, k) \mid k \in K\}$ G. (2 points)
(iv) Show H' is normal in $H \rtimes_\phi K$ and $H' \cap K' =$ identity in $H \rtimes_\phi K$. (2 points)
(v) Prove that for all $h' \in H'$ and $k' \in K'$, $(k \cdot h)' = k' h' (k')^{-1}$. (2 points)

Solution. For (i), $e_K \cdot h = \phi(e_K)(h) = id(h) = h$, for all $h \in H$, since ϕ is a group homomorphism. For $ab \in K$ and $h \in H$, $ab \cdot k = \phi(ab)(h) = \phi(a)(\phi(b)(h)) = a \cdot \phi(b)(h) = a \cdot (b \cdot h)$, so that K acts on H.

For (ii), for simplicity let us denote by 1 the identity element in each of H and K. Then we have

$$(1, 1)(h, k) = (1(1 \cdot h), 1k) = (h, k) = (h(1 \cdot e_H), k1) = (h, k)(1, 1),$$

showing that $(1, 1)$ is an identity element. Moreover, given $(h, k) \in H \rtimes_\phi K$, let $h' \in H$ be such that $\phi(k)(h') = h^{-1}$. We can do this, since $\phi(k)$ is an automorphism of H. Thus,

$$\begin{aligned}
(h, k)(h', k^{-1}) &= (h\phi(k)(h'), 1) \\
&= (hh^{-1}, 1) \\
&= (1, 1) = (h'(h')^{-1}, 1) \\
&= (h'\phi(k)^{-1}(h), 1) \\
&= (h'k^{-1} \cdot h, k^{-1}k) \\
&= (h', k^{-1})(h, k)
\end{aligned}$$

so inverses exist.

Now take $(h, k), (a, b), (c, d) \in H \rtimes_\phi K$. Then, on the one hand,

$$\begin{aligned}
(h, k)\{(a, b)(c, d)\} &= (h, k)(a\phi(b)(c), bd) \\
&= (h\phi(k)(a\phi(b)(c)), k(bd)) \\
&= (h\phi(k)(a)\phi(k)(\phi(b)(c)), k(bd)),
\end{aligned}$$

since $\phi(k)$ is a group homomorphism. On the other hand,

$$\begin{aligned}
\{(h, k)(a, b)\}(c, d) &= (h\phi(k)(a), kb)(c, d) \\
&= (h\phi(k)(a)\phi(kb)(c), (kb)d) \\
&= (h\phi(k)(a)\phi(k)(\phi(b)(c)), (kb)d)
\end{aligned}$$

since $\phi(kb)(c) = \phi(k)(\phi(b)(c))$, which shows multiplication in $H \rtimes_\phi K$ is associative (since $k(bd) = (kb)d$ in K). Thus $H \rtimes_\phi K$ is a group.

For (iii), define $\phi : H \to H'$ by $\alpha(h) = (h, 1)$. Since $(h_1, 1)(h_2, 1) = (h_1(1 \cdot h_2), 1) = (h_1h_2, 1)$, α is a group homomorphism which is clearly 1-1 and onto. Now define $\psi : K \to K'$ by $\phi(k) = (1, k)$. Then

$$(1, k_2)(1, k_2) = (1(k_1 \cdot 1), k_1k_2) = (1, k_1k_2),$$

since $k_1 \cdot 1 = 1$ because $\phi(k_1)(1) = 1$. Thus, ψ is a group homomorphism which is clearly 1-1 and onto.

For (iv), $H' \cap K' = (1, 1)$, which is the identity element of $H \rtimes_\phi K$. Now consider $(h, k)^{-1}(h_0, 1)(h, k)$. We have

$$(h, k)^{-1}(h_0, 1)(h, k) = (h, k)^{-1}(h_0(1 \cdot h), k) = (h, k)^{-1}(h_0h, k) = (h', k^{-1})(h_0h, k) = (h'(k^{-1} \cdot h_0h), 1) \in H'$$

where $(h, k)^{-1} = (h', k^{-1})$, for some $h' \in H$ as in part (ii). Thus, H' is normal in $H \rtimes_\phi K$.

For (v), on the one hand, $(k \cdot h)' = (\phi(k)(h))' = (\phi(k)(h), 1)$. On the other hand,

$$\begin{aligned} k'h'(k')^{-1} &= (1, k)(h, 1)(1, k^{-1}) \\ &= (1(k \cdot h), k)(1, k^{-1}) \\ &= (\phi(k)(h), k)(1, k^{-1}) \\ &= (\phi(k)(h)(k \cdot 1), 1) \\ &= (\phi(k)(h), 1), \end{aligned}$$

which gives what we want, since $k \cdot 1 = 1$. □

6. Let G be a group with subgroups H, K satisfying: H is normal in G, $H \cap K = \{e\}$ and $G = HK$. For $k \in K$, let $\tau_k : H \to H$ be conjugation by k.

(i) Show that $\tau_k \in \mathrm{Aut}(H)$ and $\phi : K \to \mathrm{Aut}(H)$, given by $\phi(k) = \tau_k$, is a group homomorphism. (3 points)
(ii) Prove that $G \cong H \rtimes_\phi K$. (5 points)
(iii) Show that S_3 is isomorphic to $\mathbb{Z}_3 \rtimes_\phi \mathbb{Z}_2$, for some $\phi : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$. (2 points)

Solution. For (i), we take $h, h' \in H$. Then $\tau_k(hh') = k(hh')k^{-1} = khk^{-1}kh'k^{-1} = \tau_k(h)\tau_k(h')$, so that τ_k is a group homomorphism from H to H. It is easy to see that the kernel of τ_k is the identity, so τ_k is 1-1. Finally, if $h \in H$, $k^{-1}hk \in H$, since H is normal, so that $\tau_k(k^{-1}hk) = kk^{-1}hkk^{-1} = h$, showing that τ_k is onto. Thus, τ_k is an automorphism of H. To see that ϕ is a group homomorphism, see part (ii) below.

For (ii), We first note that $\phi : K \to \mathrm{Aut}(H)$ given by $\phi(k) = \tau_k$ is a group homomorphism. For this, it suffices to show that for all $k_1, k_2 \in K$, $\tau_{k_1k_2} = \tau_{k_1}\tau_{k_2}$ as elements of $\mathrm{Aut}(H)$. For any $h \in H$ we have

$$\tau_{k_1k_2}(h) = k_1k_2h(k_1k_2)^{-1} = k_1k_2hk_2^{-1}k_1^{-1} = k_1\tau_{k_2}(h)k_1^{-1} = \tau_{k_1}(\tau_{k_2}(h)),$$

which gives what we want.

Before defining a group homomorphism between G and $H \rtimes_\phi K$, we need to see how multiplication in G works. Given $hk, h_1k_1 \in G = HK$, we have $hkh_1k_1 = (hh_1')(kk_1)$, where $kh_1 = h_1'k$, for some $h_1' \in K$, since H is normal in G. Thus, $h_1' = khk^{-1}$, so we have

$$hkh_1k_1 = h(kh_1k^{-1})(kk_1), \qquad (*)$$

which look like a semi-direct product.

Suppose now that $h_1k_1 = h_2k_2$, with $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then, $h_2^{-1}h_1 = k_2k_1^{-1}$ belongs to $H \cap K = \{e\}$. Thus, $h_2^{-1}h_1 = e = k_2k_1^{-1}$, showing $h_1 = h_2$ and $k_1 = k_2$. Thus, every element in G can be written uniquely in the form hk, with $h \in H$ and $k \in K$.

Let $\phi : K \to \mathrm{Aut}(H)$ be as above, and define $\psi : G \to H \rtimes_\phi K$ by $\psi(hk) = (h, k)$, for all $hk \in HK = G$. By the preceding paragraph, ψ is well defined. Take $hk, h_1k_1 \in G$. Then, using (*) above, we have

$$\psi((hk)(h_1k_1)) = \psi(h(k^{-1}h_1k)(kk_1)) = (hkh_1k^{-1}, kk_1) = (h\phi(k)(h_1), kk_1) = (h, k)(h_1k_1) = \psi(hk)\psi(h_1k_1),$$

showing that ψ is a group homomorphism. Since the kernel of ψ is clearly $\{e\}$ and ψ is clearly onto, we have that ψ is an isomorphism of groups, which give what we want.

For (iii), we let $G := S_3$, $H := \langle(1, 2, 3)\rangle$ and $K := \langle(1, 2)\rangle$. Then G, H, K satisfy the conditions in the statement of problem 6. Thus, $G \cong H \rtimes_\phi K$, where ϕ is defined as in (ii). Since $H \cong \mathbb{Z}_3$ and $K \cong \mathbb{Z}_2$, this gives the result.

7. 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. (10 points)

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 $a_1 C_{S_n}(\sigma), \ldots, a_r C_{S_n}(\sigma)$ 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 $a_1 C_{S_n}(\sigma), \ldots, a_r C_{S_n}(\sigma), \gamma_1 C_{S_n}(\sigma), \ldots, \gamma_r C_{S_n}(\sigma)$ 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 $C_{S_n}(\sigma) \not\subseteq A_n$. 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. □

8. Prove that the two-cycles $(1,2), (2,3), \ldots, (n-1,n)$ generate S_n. (10 points)

Solution. Since every permutation in S_n is a product of two-cycles, it suffices to show that any (i,j) with $i < j \leq n$ is a product of two-cycles from the given collection. This is clearly true for $(i, i+1)$. Suppose by induction (i,j) is a product of two-cycles from the given collection. Then $(j,j+1)(i,j)(j,j+1) = (i,j+1)$ shows that $(i,j+1)$ is a product of two-cycles from the given collection, which is what we want. □

9. Verify the class equation for S_4 and A_5. (10 points)

Solution. We use problems 2 and 7. For S_4, by problem 2, the conjugacy classes correspond to cycle types. So let $\sigma \in S_4$, There are $\binom{4}{2} = 6$ two-cycles, so $|c((1,2))| = 6$. There are 8 three-cycles, so $|c((1,2,3))| = 8$. There are three permutations that are products of two disjoint two-cycles, so $|c((1,2)(3,4))| = 3$. There are six four-cycles. To see this note that the cycles $(1,a,b,c)$ are all distinct, where a,b,c is a permutation of $2,3,4$. Thus, $|c((1,2,3,4))| = 6$. We have so far accounted for $6+8+3+6 = 23$ elements in S_4. Only e is left, which also shows $|Z(S_4)| = 1$. Thus,

$$\begin{aligned} 24 = |S_4| &= 1 + 6 + 8 + 3 + 6 \\ &= |Z(S_4)| + |c((1,2))| + |c((1,2,3))| + |c((1,2)(3,4))| + |c((1,2,3,4))| \end{aligned}$$

where we have accounted for all elements whose conjugacy class contains more than one element.

We repeat the same analysis for A_5, but using both problems 2 and 7. Let $X = \{1,2,3,4,5\}$. If we are given four elements $a,b,c,d \in X$, we may form three even permutations from them that are products of two disjoint two-cycles. Doing this for all five choices of a,b,c,d, we have that $|c((1,2)(3,4))| = 15$, where $c((1,2)(3,4))$ denotes the conjugacy class of $(1,2)(3,4)$ in S_5. Since $(1,2)$ commutes with $(1,2)(3,4)$, the centralizer of $(1,2)(3,4)$ is not contained in A_5, so by problem 7, $c((1,2)(3,4)) = c_{A_5}((1,2)(3,4))$, and thus $|c_{A_5}((1,2)(3,4))| = 15$.

There are 20 three-cycles in S_5, so that $|c((1,2,3))| = 20$. Since $(4,5)$ is an odd cycle commuting with $(1,2,3)$, problem 7 gives $20 = |c_{A_5}((1,2,3))|$.

Now consider the five-cycle (1,2,3,4,5). By problem 2, the centralizer of (1,2,3,4,5) is $\langle(1,2,3,4,5)\rangle \subseteq A_5$. Thus, by problem 7, $c((1,2,3,4,5) = c_{A_5}((1,2,3,4,5)) \cup c_{A_5}((1,2)(1,2,3,4,5)(1,2))$. Note that $(1,2)(1,2,3,4,5)(1,2) = (1,3,4,5,2)$. Since there are $4! = 24$ five-cycles in S_5, by problem 2, $c((1,2,3,4,5))| = 24$, and thus, by problem 7, $|c_{A_5}((1,2,3,4,5))| = 12 = |c_{A_5}((1,3,2,4,5))|$.

We have now accounted for $15+20+12+12 = 59$ elements in A_5. This leaves just e, showing $|Z(A_5)| = 1$. Therefore, we have

$$\begin{aligned} 60 = |A_5| &= 1 + 15 + 20 + 12 + 12 \\ &= |Z(G)| + |c_{A_5}((1,2)(3,4))| + |c_{A_5}((1,2,3))| + |c_{A_5}((1,2,3,4,5))| + |c_{A_5}(((1,3,4,5,2))|, \end{aligned}$$

thereby verifying the class equation for A_5.

10. 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? (10 points)

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 $[G : C_G(x_i)] = p^2$, it would then follow that $Z(G) = C_G(x_i)$, which is a contradiction, since $x_i \notin Z(G)$. Thus, each $[G : C_G(x_i)] = p$. Therefore, $p^3 = p + rp$, which implies $r = p^2 - 1$. □

Bonus Problem. For $n \geq 5$, show that A_n is the only proper normal subgroup of S_n. This problem must be correct to receive any credit.

Solution. We follow the path laid out in Homework 8.

(i) Let G be a group and A, B normal subgroups of G. Then $A \cap B$ is a normal subgroup. Conclude that if A is a simple group, then $A \cap B = \{e\}$. 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). 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. 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 $b_1 A = b_2 A$, 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). Let G be a group and $B = \{e, b\}$ a normal subgroup of order two. Then $b \in Z(G)$, the center of G. This follows, since, for all $g \in g$, $g^{-1} b g = b$, so $bg = gb$, i.e., $b \in Z(G)$.

(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. 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 $Z(S_n) = \{e\}$. For this, it suffices to show that if $\sigma \in S_n$, then there exists $\tau \in S_n$ such that $\sigma\tau \neq \tau\sigma$. Take $i, j \in X_n$ such that $i \neq j$ and $\sigma(i) = j$. Take $k \neq i, j$, and set $\tau = (j, k)$. Then, $\tau\sigma(i) = \tau(j) = k$. On the other hand, $\sigma\tau(i) = \sigma(i) = j$. Thus, σ and τ do not commute, showing $Z(S_n) = \{e\}$. □.