1 Problem 1

Recall that any two elements of $S_n$ are conjugate if and only if they have the same cycle type. It therefore suffices to enumerate the cycle types of $S_n$ for $n \leq 4$, and the elements of $S_n$ which have this cycle type.

(1) $S_1$: Note that $S_1 = \{e\}$, so there is only one conjugacy class, the trivial cycle $c_1 = \{e\}$.

(2) $S_2$: The elements of $S_2$ are the identity and the transposition which swaps the two elements, i.e. $S_2 = \{e, (12)\}$ in cycle notation. The possible conjugacy classes are therefore $c_1 = \{e\}$ and $c_2 = \{(12)\}$.

(3) $S_3$: Note $S_3 = \{e, (12), (23), (13), (123), (132)\}$, so the only possible cycle types are the identity, transpositions, and 3-cycles, each sharing their own conjugacy class. Therefore, the possible conjugacy classes are:

$$c_1 = \{e\}, c_2 = \{(12), (23), (13)\}, c_3 = \{(123), (132)\}$$

(4) $S_4$: The possible elements of $S_4$ are $k$-cycles for $1 \leq k \leq 4$, and products of disjoint transpositions. Hence, the possible cycle types are (1), (2), (3), (4), and (2, 2). This gives 5 conjugacy classes, which we enumerate explicitly below:

$$c_1 = \{e\}; c_2 = \{(12), (13), (14), (23), (24), (34)\}$$

$$c_3 = \{(123), (134), (132), (143), (234), (243), (124), (142)\}$$

$$c_4 = \{(1234), (1432), (1324), (1342), (1423), (1243)\}$$

$$c_{2,2} = \{(12)(34), (14)(23), (13)(24)\}$$

2 Problem 2

As always, $\{e\}$ and $A_4$ are trivially subgroups of $A_4$. Note that

$$A_4 = \{e, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}$$

Each element of order 2, i.e. the products of disjoint transpositions, generates a unique cyclic subgroup of $A_4$ of order 2. The 3-cycles generate 4 unique cyclic subgroups of order 3, namely $\langle (123) \rangle$, $\langle (124) \rangle$, $\langle (134) \rangle$, and $\langle (234) \rangle$. Finally, a small number of multiplications shows that the set of all products of disjoint transpositions, $V = \{e, (12)(34), (13)(24), (14)(23)\}$ form a subgroup of $A_4$ of order 4 (in fact, since conjugation preserves cycle type, $V$ is in fact a normal subgroup of $A_4$). We can think of $V$ as the subgroup of $A_4$ generated by any two distinct double transpositions. We claim that these are the only proper subgroups of $A_4$, and in particular that $A_4$ has no subgroup of order 6.

For this, it suffices to show that any subgroup of $A_4$ containing a double transposition and a 3-cycle must be all of $A_4$. We appeal to Lagrange’s theorem here: any subgroup of $A_4$ must
have order dividing $|A_4| = 12$, so if a 3-cycle and a double transposition generate more than 6 elements, any subgroup which contains both must be all of $A_4$. Now, we compute:

$$(123)((12)(34)) = (134)$$

$$(134)((12)(34)) = (124)$$

$$(124)((12)(34)) = (143)$$

$$(143)((12)(34)) = (124)$$

$$(142)((12)(34)) = (243)$$

$$(234)((12)(34)) = (132)$$

$$(132)((12)(34)) = (234)$$

$$(243)((12)(34)) = (134)$$

Hence, the above computations show that if any subgroup of $A_4$ contains any 3-cycle and $(12)(34)$, then it contains all eight 3-cycles, and thus must be all of $A_4$. We make similar computations below:

$$(123)((13)(24)) = (243)$$

$$(134)((13)(24)) = (142)$$

$$(124)((13)(24)) = (132)$$

$$(143)((13)(24)) = (234)$$

$$(142)((13)(24)) = (134)$$

$$(234)((13)(24)) = (143)$$

$$(132)((13)(24)) = (124)$$

$$(243)((13)(24)) = (123)$$

Therefore, if any subgroup of $A_4$ contains any 3-cycle and $(13)(24)$, then it contains all eight 3-cycles, and thus must be all of $A_4$. Finally, we see

$$(123)((14)(23)) = (142)$$

$$(134)((14)(23)) = (243)$$

$$(124)((14)(23)) = (234)$$

$$(143)((14)(23)) = (132)$$

$$(142)((14)(23)) = (123)$$

$$(234)((14)(23)) = (124)$$

$$(132)((14)(23)) = (143)$$

$$(243)((14)(23)) = (134)$$
Therefore, if any subgroup of $A_4$ contains any 3-cycle and $(14)(23)$, then it contains all eight 3-cycles, and thus must be all of $A_4$. This proves the claim that any subgroup which contains 3-cycle and any double transposition must be all of $A_4$. It remains to show that any subgroup of $A_4$ containing two 3-cycles which generate distinct cyclic subgroups must be all of $A_4$. To this end, we show that the subgroup generated by any two such 3-cycles contains a double transposition, proving the claim and completing the proof. It suffices to do this for the specified generators for each cyclic subgroup of order 3.

$$(123)(124) = (13)(24)$$

$$(123)(134) = (234)$$

$$(123)(234) = (12)(34)$$

$$(134)(234) = (13)(24)$$

$$(124)(134) = (13)(24)$$

$$(124)(234) = (123)$$

Hence, the subgroups of $A_4$ are

$$\{\{e\}, \langle(12)(34)\rangle, \langle(13)(24)\rangle, \langle(14)(23)\rangle, \langle(123)\rangle, \langle(124)\rangle, \langle(134)\rangle, \langle(234)\rangle, V, A_4\}$$

### 3 Problem 3

(a) Since every element of $S_n$ can be written as a product of transpositions, it follows that $S_n$ is generated by the set of all transpositions. Hence, it suffices to show that every transposition is in the subgroup $S$ generated by the $(1,2), (1,3), (1,4), \ldots, (1,n)$. Every transposition of the form $(1,k)$ is clearly in $S$, so it remains to show that any transposition of the form $(i,j) \in S$ for $i \neq j$ and $i \neq j \neq 1$. We see that

$$(1, i)(1,j)(1,i) = (1,i)(1,i,j) = (i,j)$$

so the transposition $(i,j)$ is in the $S$, which completes the proof.

(b) Let $K$ be the subgroup of $S_n$ generated by the cycles $(1,2)$ and $(1,2,\ldots,n)$. We want to show $K = S_n$. We first prove that the subgroup $H$ generated by elements $(1,2), (2,3),\ldots,(n,n-1)$ is all of $S_n$. To this end, we claim that $(1,j) \in H$ for all $2 \leq j \leq n$. We proceed by induction. The case $j = 2$ is clear, so suppose our hypothesis is true $j > 2$; we want to show the hypothesis is true for the case $j + 1$. Note that $(1,j) \in H$ by hypothesis, so

$$(1,j)(j,j+1)(1,j) = (1,j+1) \in H$$

This completes the induction. Hence, by (a), $H = S_n$. Thus, it suffices to show that $(i,i+1) \in K$ for each $i \in \{1,\ldots,n-1\}$. We claim that for all $k \in \{0,\ldots,n-2\}$,

$$(1,2,\ldots,n)^k(1,2,\ldots,n)^{-k} = (k + 1, k + 2)$$
We proceed by induction. The base case is clear, as
\[(1, 2, \ldots, n)^0(1, 2)(1, 2, \ldots, n)^{-0} = e(1, 2)e = (1, 2) = (0 + 1, 0 + 2)\]
Suppose the claim is true for \(k > 0\); we want to show the hypothesis is true for the case \(k + 1\). By the induction hypothesis, we see
\[(1, 2, \ldots, n)^{k+1}(1, 2)(1, 2, \ldots, n)^{-(k+1)} = (1, 2, \ldots, n)^1(k+1,k+2)(1, 2, \ldots, n)^{-1} = (k+2,k+3)\]
which completes the induction. Hence, \(K = S_n\), as desired.

4 Problem 4

Let \(n \geq 3\). We claim \(S_n\) has trivial center. Let \(\sigma \neq e \in S_n\). Let \(i \in \{1, \ldots, n\}\) such that \(\sigma(i) = j \neq i\) for some \(j \in \{1, \ldots, n\}\). Since \(\sigma\) is a bijection, \(\sigma(l) \neq j\) for any \(l \neq i\). Let \(\gamma \in S_n\) be the transposition which interchanges \(i\) and some \(k \neq j\); this is possible since \(n \geq 3\). Then note that
\[\sigma(\gamma(i)) = \sigma(k) \neq j\]
but
\[\gamma(\sigma(i)) = \gamma(j) = j\]
Since \((\sigma \circ \gamma)(i) \neq (\gamma \circ \sigma)(i)\), it follows \(\gamma \sigma \neq \sigma \gamma\). Hence, no nontrivial element of \(S_n\) commutes with every element of \(S_n\), so \(Z(S_n) = \{e\}\).

Let \(n \geq 4\). We claim \(A_n\) has trivial center. Let \(\sigma \neq e \in A_n\). Let \(i \in \{1, \ldots, n\}\) such that \(\sigma(i) = j \neq i\) for some \(j \in \{1, \ldots, n\}\). Put \(l = \sigma^{-1}(i) \in \{1, \ldots, n\}\), and let \(k \in \{1, \ldots, n\}\) such that \(k \neq l, i, j\); this is possible since \(n \geq 4\). Since \(\sigma\) is a bijection, \(\sigma(k) \neq i\) since \(k \neq l\). Put \(\gamma = (i,k,j) \in A_n\). Then
\[\gamma(\sigma(i)) = \gamma(j) = i\]
but
\[\sigma(\gamma(i)) = \sigma(k) \neq i\]
since \(k \neq l\). Since \((\sigma \circ \gamma)(i) \neq (\gamma \circ \sigma)(i)\), it follows \(\gamma \sigma \neq \sigma \gamma\). Hence, no nontrivial element of \(A_n\) commutes with every element of \(A_n\), so \(Z(A_n) = \{e\}\).

5 Problem 5

(a) See the proof that \(Z(A_n)\) is trivial for \(n \geq 4\) provided in problem 4. The proof given in fact shows that the centralizer of \(A_n\) in \(S_n\) is trivial, with the small modification that the initial sigma can be any nontrivial element of \(S_n\), as the element \(\gamma\) which does not commute with \(\sigma\) is an element of \(A_n\).

(b) Let \(g \in S_n\) be an odd transformation, and consider the map \(f: A_n \to A_n\) given by \(f(x) = gxg^{-1}\). Note that \(f\) is a homomorphism, as for any \(x, y \in A_n\),
\[f(xy) = gxg^{-1} = gx(g^{-1}g)yg^{-1} = f(x)f(y)\]
Further, since conjugation preserves cycle type, \( g^{-1}xg \in A_n \) for any \( x \in A_n \). Let \( x \in A_n \); then \( f(g^{-1}xg) = gg^{-1}xgg^{-1} = x \), so \( f \) is surjective. Since \( A_n \) is finite, \( f \) is also injective, whence \( f \) is an automorphism.

Let \( n \geq 4 \), and suppose \( f \) is an inner automorphism, seeking a contradiction. Then \( f(x) = yxy^{-1} \) for some \( y \in A_n \) for all \( x \in A_n \), so in particular, \( gxg^{-1} = yxy^{-1} \) for all \( x \in A_n \). Equivalently, \( y^{-1}gx = xy^{-1}g \) for all \( x \in A_n \), i.e. \( y^{-1}g \) is in the centralizer of \( A_n \) in \( S_n \). By part (a), the centralizer of \( A_n \) in \( S_n \) is trivial, i.e. \( y^{-1}g = e \), or \( y = g \), a contradiction as \( g \notin A_n \) by hypothesis.

Suppose \( n = 3 \). Then \( A_3 \) is cyclic, so \( \text{Inn}(A_3) \) is trivial. It suffices then to show that \( f: A_3 \to A_3 \) given by \( f(x) = gxg^{-1} \) is a nontrivial automorphism for any transposition \( g \in S_3 \). This is clear, as

\[
(12)(123)(12)^{-1} = (12)(123)(12) = (12)(13) = (132) \\
(23)(123)(23)^{-1} = (23)(123)(23) = (23)(12) = (132)
\]

This completes the proof.

6 Problem 6

Let \( f \in \text{Aut}(S_3) \). Since automorphisms preserve order, it follows that \( f((123)) \) is a 3-cycle and \( f((12)) \) is a 2-cycle. Since there are two 3-cycles in \( S_3 \) and three 2-cycles in \( S_3 \), it follows that \( |\text{Aut}(S_3)| \leq 6 \). By problem 4, \( Z(S_3) = \{e\} \), so \( S_3/Z(S_3) \cong \text{Inn}(S_3) \cong S_3 \). Hence, \( |\text{Inn}(S_3)| = 6 \), and since \( \text{Inn}(S_3) \subseteq \text{Aut}(S_3) \), we have \( \text{Aut}(S_3) = \text{Inn}(S_3) \cong S_3 \).

7 Problem 7

Note that \( |S_5| = 120 = 2^3 \cdot 3 \cdot 5 \), so there are three Sylow \( p \)-subgroups to be considered: the Sylow 2-subgroups of order 8, the Sylow 3-subgroups of order 3, and the Sylow 5-subgroups of order 5. Denote the number of Sylow \( p \)-subgroups by \( n_p \). We tackle each case separately. By the 3rd Sylow theorem, \( n_3 \) divides 40 and \( n_3 \equiv 1 \pmod{3} \). Enumerating the divisors of 40, we see that the only possible values are \( n_3 = 40, n_3 = 10, n_3 = 4, \) and \( n_3 = 1 \). Since every two distinct Sylow 3-subgroups are of order 3, they must intersect trivially. Hence, if \( n_3 = 40 \), then that implies there are 80 elements of order 3 in \( S_5 \), which is clearly false. Since every element of order 3 is contained in a Sylow 3-subgroup, if \( n_3 \leq 4 \), then there can be at most 8 elements of order 3 in \( S_5 \). But there are clearly more, as exhibited by the following 9 elements:

\[
\{(123), (132), (124), (142), (134), (143), (234), (243), (135)\} \subseteq S_5
\]

Hence, there are 10 Sylow 3-subgroups in \( S_5 \), each of order 3. Since every group of order 3 is isomorphic to the cyclic group of order 3, each Sylow 3-subgroup of \( S_5 \) is cyclic.

By the 3rd Sylow theorem, \( n_5 \) divides 24 and \( n_5 \equiv 1 \pmod{5} \). Enumerating the divisors of 24, we see that the only possible values are \( n_5 = 6, \) and \( n_5 = 1 \). Since every element of
order 5 is contained in a Sylow 5-subgroup, if \( n_5 = 1 \), then there can be at most 4 elements of order 5 in \( S_5 \). But there are clearly more, as exhibited by the following 5 elements:

\[
\{(12345), (13452), (14523), (15234), (14235)\} \subset S_5
\]

Hence, there are 6 Sylow 5-subgroups in \( S_5 \), each of order 5. Since every group of order 5 is isomorphic to the cyclic group of order 5, each Sylow 5-subgroup of \( S_5 \) is cyclic. By the 3rd Sylow theorem, \( n_5 \) divides 15 and \( n_5 \equiv 1 \pmod{2} \). Enumerating the divisors of 15, we see that the only possible values are \( n_5 = 15, n_5 = 5, n_5 = 3, \) and \( n_5 = 1 \). Since every element of order 2 or 4 is contained in a Sylow 2-subgroup, if \( n_2 \leq 5 \), then there can be at most 35 elements of order 2 or 4 in \( S_5 \). But there are more, as exhibited by the following 36 elements:

\[
(12), (13), (14), (15), (23), (24), (25), (34), (35), (45) \quad (10 \text{ elements})
\]

\[
(12)(34), (12)(35), (12)(45), (13)(24), (13)(25), (13)(45) \quad (6 \text{ elements})
\]

\[
(14)(23), (14)(25), (14)(35), (15)(23), (15)(24), (15)(34) \quad (6 \text{ elements})
\]

\[
(23)(45), (24)(35), (25)(34) \quad (3 \text{ elements})
\]

\[
(1234), (1243)(1324), (1342), (1423), (1432) \quad (6 \text{ elements})
\]

\[
(1235), (1253)(1325), (1352), (1523) \quad (5 \text{ elements})
\]

Hence, there are 15 Sylow 2-subgroups in \( S_5 \), each of order 8. Since every two Sylow 2-subgroups are conjugate by an element of \( S_5 \), hence isomorphic, it suffices to determine the isomorphism type of just one of the Sylow 2-subgroups. Note that \( S = \langle (13), (1234) \rangle \) is a subgroup of \( S_5 \) with 8 elements, so \( S \) is a Sylow 2-subgroup of \( S_5 \). Since \( (1234)(13) = (14)(23) = (13)(1432) = (13)(1234)^{-1} \), there is an obvious isomorphism between \( S \) and \( D_4 \), the dihedral group of order 8, so we see that every Sylow 2-subgroup of \( S_5 \) is isomorphic to \( D_4 \). Alternatively, note that \( D_4 \) embeds straight-forwardly into \( S_4 \) as the symmetry group of the square, permuting the 4-vertices. Since \( S_4 \) embeds into \( S_5 \), it is clear that there is a subgroup of order 8 of \( S_5 \) which is isomorphic to \( D_4 \). By the argument above, this implies every Sylow 2-subgroup of \( S_5 \) is isomorphic to \( D_4 \).

8 Problem 8

Note that the claim is trivial for the cases \( n = 1, 2 \), as the only subgroup of index \( n \) in \( S_n \) is \( \{e\} \) for \( n = 1, 2 \). The claim is true for \( n = 3 \), as any subgroup of \( S_3 \) index 3 has order 2, and is hence isomorphic to \( S_2 \) (all groups of order 2 are isomorphic). Hence, it suffices to take \( n \geq 4 \). Let \( H \) be a subgroup of \( S_n \) of index \( n \), and consider the homomorphism \( \varphi : S_n \to S(X) \) given by the left action of \( S_n \) on the set \( X = S_n/H \) of cosets of \( H \) in \( S_n \). Suppose \( g \in \ker(\varphi) \). Then we must have \( \varphi(g)(H) = gH = H \), i.e. \( g \in H \), so \( \ker(\varphi) \subseteq H \). We split into two cases.

Suppose \( n = 4 \). Then since \( \ker(\varphi) \) is a normal subgroup of \( S_4 \), it must be \( \{e\}, V_4, A_4, \) or \( S_4 \). Since the latter have index 2 and 1 in \( S_n \) respectively, and \( [G : \ker(\varphi)] \geq [S_4 : H] = 4 > 2 \), we must have \( \ker(\varphi) = \{e\} \) or \( \ker(\varphi) = V_4 \). Since \( \ker(\varphi) \) is a subgroup of \( H \), its order divides \( |H| \) by Lagrange. Since \( [S_4 : H] = 4 \), we have \( |H| = 6 \); since \( |V_4| = 4 \) does not divide 6, we
must have have ker(φ) = {e} i.e. φ is injective.
Suppose n ≥ 5. Note K := ker(φ) is a normal subgroup of S_n. We claim K must be {e}, A_n, or S_n. Note that since K ⊆ S_n, K ∩ A_n is a normal subgroup of A_n. Since A_n is simple for n ≥ 5, we must have K ∩ A_n = 1 or K ∩ A_n = A_n. In the latter case, A_n ⊆ K, and since [S_n : A_n] = 2, this implies K = A_n or K = S_n. Suppose K ∩ A_n = 1. Then if K has at least two distinct nonidentity elements σ, τ which are both odd, either σ^2 ≠ e or στ ≠ e, both of which are even, a contradiction. Hence, |K| ≤ 2. But K ≤ G; since conjugation always fixes the identity, this means K ⊆ Z(S_n). Since we proved Z(S_n) = {e} for n ≥ 3 in problem 4, we must have K = {e}.
Hence, ker(φ) is one of {e}, A_n or S_n. Since the latter two have index 2 and 1 in S_n respectively, and [G : ker(φ)] ≥ [S_n : H] = n > 2, we must have ker(φ) = {e}, i.e. φ is injective. In either case, since |X| = n, it follows that |S(X)| = n! = |S_n|, so φ is also surjective, i.e. φ is an isomorphism. It follows that H is isomorphic to its image under φ. Note that φ(g)(H) = gH = H if and only if g ∈ H, so φ(H) is precisely the set of elements of S(X) which fix the element H ∈ X. The subgroup of elements of S_n which fix a single element is isomorphic to S_{n-1}, so H ≅ φ(H) ≅ S_{n-1}.

9 Problem 9

(a) The claim is trivially true for n = 1, 2, since A_n = {e} in these cases. In the case n = 3, A_3 is the cyclic group of order 3, so the only proper subgroup of A_3 is trivial and thus has index 3. Suppose n ≥ 5.
Let H be a proper subgroup of A_n of index k > 1, and consider the homomorphism φ: A_n → S(X) given by the left action of A_n on the set X = A_n/H of cosets of H in A_n. Note |X| = k, so S(X) ≅ S_k. Suppose g ∈ ker(φ). Then we must have φ(g)(H) = gH = H, i.e. g ∈ H, so ker(φ) ⊆ H. Since ker(φ) is a normal subgroup of A_n, it must be {e} or A_n by the simplicity of A_n. Since ker(φ) ⊆ H ⊆ A_n, we must have ker(φ) = {e}, i.e. φ is injective homomorphism from A_n → S_k. Hence, we must have |S_k| ≥ |A_n|, i.e. 2 · k! > n!; since n ≥ 5, we must have k ≥ n.
(b) Suppose there were an injective homomorphism φ: S_n → A_{n+1} for n ≥ 2. Then S_n ≅ Im(φ), which is necessarily a subgroup of A_{n+1}. But then

\[ [A_{n+1} : \text{Im}(φ)] = \frac{|A_{n+1}|}{|S_n|} = \frac{(n+1)!}{2n!} = \frac{(n+1)}{2} < n \]

a contradiction by part (a).

10 Problem 10

(a) Let n ≥ 1, and let φ: S_n → A_{n+2} be defined as follows:

\[ φ(σ) = \begin{cases} σ & \text{if sgn}(σ) = 1 \\ σγ & \text{if sgn}(σ) = -1 \end{cases} \]
where $\gamma$ is the transposition that interchanges $n + 1$ and $n + 2$ and sgn is the sign homomorphism. Note that the codomain of $\varphi$ is indeed $A_{n+2}$, as if $\text{sgn}(\sigma) = -1$, then since $\text{sgn}(\gamma) = -1$ and sgn is a homomorphism, we have

$$\text{sgn}(\sigma \gamma) = \text{sgn}(\sigma) \text{sgn}(\gamma) = (-1)^2 = 1$$

We need to show that $\varphi$ is an injective homomorphism. Let $\sigma, \tau \in S_n$. If $\text{sgn}(\sigma) = \text{sgn}(\tau) = 1$, then $\text{sgn}(\sigma \tau) = 1$, so

$$\varphi(\sigma \tau) = \sigma \tau = \varphi(\sigma) \varphi(\tau)$$

Suppose $\text{sgn}(\sigma) = 1, \text{sgn}(\tau) = -1$. Then $\text{sgn}(\sigma \tau) = -1$, so

$$\varphi(\sigma \tau) = \sigma \tau \gamma = \sigma (\tau \gamma) = \varphi(\sigma) \varphi(\tau)$$

Suppose $\text{sgn}(\sigma) = -1, \text{sgn}(\tau) = 1$. Then $\text{sgn}(\sigma \tau) = -1$, and since $\gamma$ is disjoint from $\sigma$ and $\tau$, it commutes with both $\sigma$ and $\tau$, so

$$\varphi(\sigma \tau) = \sigma \tau \gamma = \sigma \gamma \tau = (\sigma \gamma) \tau = \varphi(\sigma) \varphi(\tau)$$

Finally, suppose $\text{sgn}(\sigma) = -1, \text{sgn}(\tau) = -1$. Then $\text{sgn}(\sigma \tau) = 1$, and as above, $\gamma$ is disjoint from $\sigma$ and $\tau$, it commutes with both $\sigma$ and $\tau$, so

$$\varphi(\sigma \tau) = \sigma \tau = \sigma \tau \gamma^2 = \sigma \tau \gamma \gamma = (\sigma \gamma)(\tau \gamma) = \varphi(\sigma) \varphi(\tau)$$

Hence, $\varphi$ is a homomorphism. Furthermore, let $\sigma$ be any nontrivial element of $S_n$. If $\text{sgn}(\sigma) = 1$, then $\varphi(\sigma) = \sigma$, which is a nontrivial element of $A_{n+2}$. If $\text{sgn}(\sigma) = -1$, then $\varphi(\sigma) = \sigma \tau$; since $\tau$ is disjoint from $\sigma$, $\sigma \tau$ is also a nontrivial element of $A_{n+2}$. Hence, $\ker(\varphi)$ is trivial, so $\varphi$ is injective.

(b) Let $G$ be a finite group of order $n$. If $n = 1$, the theorem is trivial. If $n = 2$, note that $G$ is isomorphic to the cyclic subgroup generated by $(12)(34)$ in $A_5$, and $A_5$ simple group. Suppose $n \geq 3$. By Cayley’s theorem, $G$ is isomorphic to a subgroup of $H$ of $S_n$. By part (a), there exists an injective homomorphism $\varphi: S_n \rightarrow A_{n+2}$, so by the first isomorphism theorem, $\varphi(H)$ is isomorphic to a subgroup $K$ of $A_{n+2}$, i.e. $G \cong H \cong K$. Since $n \geq 3$, $n + 2 \geq 5$, so $A_{n+2}$ is simple. This proves every finite group is isomorphic to a subgroup of a finite simple group.