Exercises on the Symmetric Group

Baptiste Arnaudo

1 Introduction

This document is a collection of exercises about the symmetric group on n elements, including results that are useful to know before oral examinations, in particular those of École Polytechnique (“X”) for MP.

2 Exercises

Exercise 1: A power computation
Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 5 & 7 & 6 & 3 & 8 & 2 \end{pmatrix}$. Compute σ^{2023}.

Exercise 2: Degree-1 characters of S_n
Let $n \geq 2$. Determine the group homomorphisms from S_n to $(\mathbb{C}^*, \times)$.

Exercise 3: Generating S_n
Show that the transpositions $(1, k)$ for $2 \leq k \leq n$ generate S_n; likewise the adjacent transpositions $(k, k+1)$ for $1 \leq k \leq n-1$; likewise $(1\,2)$ together with $(1\,2\,\ldots\,n)$. What is the minimal number of transpositions needed to generate S_n?

Exercise 4: Generation of S_n by transpositions
Show by induction that transpositions generate S_n for $n \geq 2$.

Exercise 5: Simplicity of the alternating group for $n \geq 5$
First some definitions: a subgroup H of a group G is *normal* if

$$\forall h \in H,\ \forall g \in G,\quad ghg^{-1} \in H.$$

For example, if G is a group with identity e_G, then $\{e_G\}$ and G are normal.
A group G is *simple* if its only normal subgroups are $\{e_G\}$ and G.
Show that $\mathscr{A}_n$ (the alternating group of degree n, i.e. permutations of sign $+1$) is simple for $n \geq 5$.

Exercise 6: Cayley's theorem
Let G be a group. Show that G is isomorphic to a subgroup of $S(G)$ (the bijections from G to itself).

Exercise 7: Subgroups of S_n of index at most n for $n \geq 5$
The index of a subgroup H of a finite group G, usually denoted $[G : H]$, is the cardinality of the quotient set G/H defined as the set of equivalence classes on G for the relation

$$xRy \Longleftrightarrow y \in xH.$$

Show that if $n \geq 5$ and if H is a normal subgroup of S_n of index $2 \leq r \leq n-1$, then $r = 2$ and $H = \mathscr{A}_n$. Show that the subgroups of index n of S_n are isomorphic to S_{n-1}. You may use the simplicity of $\mathscr{A}_n$ for $n \geq 5$ to show that the only normal subgroups of S_n for $n \geq 5$ are S_n, $\mathscr{A}_n$ and $\{id\}$.

Exercise 8: Stability of $\mathscr{A}_n$ under every automorphism of S_n
Show that $\mathscr{A}_n$ is stable under every automorphism of S_n.

Exercise 9: Automorphisms of S_n for $n \neq 6$
The goal of this exercise, which I was asked in the 2023 X orals, is to show that when $n \neq 6$, every automorphism of S_n is inner (i.e. of the form $u \mapsto \sigma \circ u \circ \sigma^{-1}$ for some permutation σ).
Question 1 For $\sigma \in S_n$ write $Z(\sigma) = \{\tau \in S_n \mid \tau \circ \sigma = \sigma \circ \tau\}$ (the *centralizer* of σ). Show that $Z(\sigma)$ is a subgroup of S_n and that for every $\varphi \in \mathrm{Aut}(S_n)$, $Z(\varphi(\sigma)) = \varphi(Z(\sigma))$.
Question 2 Compute $|Z(\sigma)|$ when σ is a product of k disjoint transpositions.
Question 3 Assume $n \neq 6$. Let $\varphi \in \mathrm{Aut}(S_n)$ and τ a transposition. Show that $\varphi(\tau)$ is a transposition.
Question 4 Deduce that φ is inner.

Exercise 10: No injective group homomorphism $S_n \hookrightarrow \mathscr{A}_{n+1}$ for $n \geq 2$
Show that there is no injective group homomorphism from S_n into $\mathscr{A}_{n+1}$ for $n \geq 2$. First handle the cases $n = 2$ and $n = 3$.

3 Hints

Hints for Exercise 1:

Determine the order of σ by decomposing it into a product of disjoint cycles.

Hints for Exercise 2:

Look at the images of transpositions; use that they generate S_n.

Hints for Exercise 3:

Express transpositions (i, j) using $(1, k)$, then express $(1, k)$ using $(k, k+1)$, then express

$(k, k+1)$ using $(1,2)$ and $(1,2,\ldots,n)$. To get a feel for the last question, see what happens if you remove one of the $(1,k)$: do the remaining transpositions still generate S_n?

Hints for Exercise 4:

Argue by induction on n.

Hints for Exercise 5:

This is a hard exercise; intermediate facts are needed. First show that 3-cycles generate $\mathscr{A}_n$, then that two 3-cycles are always conjugate in $\mathscr{A}_n$. Next, take a nontrivial normal subgroup H of $\mathscr{A}_n$ and show it contains a 3-cycle by considering the disjoint cycle decomposition of an element $\sigma \in H \setminus \{id\}$ that maximizes the number of fixed points among elements of H.

Hints for Exercise 6:

Consider

$$\begin{aligned} \varphi \, : G &\to S(G) \\ g &\mapsto \varphi(g) \end{aligned}$$

where

$$\begin{aligned} \varphi(g) \, : G &\to G \\ h &\mapsto gh \end{aligned}$$

This is the *left translation action of G on itself*. When in doubt, this homomorphism is often useful.

Hints for Exercise 7:

Mimic Exercise 6 by letting S_n act on S_n/H by left translation. Note that the kernel of a group homomorphism is always a normal subgroup of the domain.

Hints for Exercise 8:

Look at the orders of the images of 3-cycles.

Hints for Exercise 9:

For the last question, consider the images under φ of $(1,k)$ for $2 \leq k \leq n$. Show by induction that there exist pairwise distinct $x_1, \ldots, x_n$ such that $\forall k \in \{2,\ldots,n\}$, $\varphi((1,k)) = (x_1, x_k)$.

Hints for Exercise 10:

Two necessary conditions for the existence of an injective homomorphism between two finite groups are: the order of the first divides that of the second, and the target has a subgroup whose order equals that of the source. Use the first for $n = 2$, and the second for $n = 3$. For the general case, argue by contradiction assuming such a morphism φ exists and take inspiration from Exercise 7.

4 Solutions

<u>**Solution to Exercise 1:**</u>

The general method for this type of problem is: **first determine the order of the element in the ambient group**, here the order of σ in S_8.

Decompose σ into a product of disjoint cycles; this decomposition exists and is unique up to the order of the factors. Such cycles commute (their supports are disjoint), and if g, h are commuting finite-order elements in a group G, then gh has finite order dividing the lcm of the orders of g and h.

To compute the disjoint cycle decomposition of $\sigma \in S_n$, compute $\sigma(1)$, then $\sigma(\sigma(1))$, etc., until you return to 1: that gives a first cycle. Then do the same starting from the smallest $k \in \{1, \ldots, n\}$ not yet encountered; this gives a second cycle. Stop when every element of $\{1, \ldots, n\}$ has appeared.

Here $\sigma(1) = 4$, $\sigma(4) = 7$, $\sigma(7) = 8$, $\sigma(8) = 2$, $\sigma(2) = 1$, so we get the cycle $(1\,4\,7\,8\,2)$, denote it by γ. Next: $\sigma(3) = 5$, $\sigma(5) = 6$, $\sigma(6) = 3$, so we get $(3\,5\,6)$, denote it by τ.
Thus $\sigma = \tau\gamma$ with τ and γ commuting, so the order of σ divides $\mathrm{lcm}(\mathrm{ord}(\tau), \mathrm{ord}(\gamma)) = \mathrm{lcm}(3, 5) = 15$. Since $2023 = 15 \times 134 + 13$, we get

$$\sigma^{2023} = \sigma^{13} = \tau^{13}\gamma^{13} = \tau\,\gamma^{-2}.$$

To compute γ^{-2}, first compute γ^2 by moving two steps in the cycle each time: $(1\,7\,2\,4\,8)$, then invert the order of the cycle to get $\gamma^{-2} = (1\,8\,4\,2\,7)$.
Hence

$$\sigma^{2023} = (3\,5\,6)(8\,4\,2\,7\,1) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 5 & 2 & 6 & 3 & 1 & 4 \end{pmatrix}.$$

<u>**Solution to Exercise 2:**</u>

This exercise showcases several important facts. If G and H are groups and $S \subset G$ generates G (i.e. $G = \langle S \rangle$), then any homomorphism $\varphi : G \to H$ is completely determined by the images of S. Moreover, if H is abelian (as is $(\mathbb{C}^*, \times)$), then φ is constant on conjugacy classes because

$$\forall g, g' \in G, \quad \varphi(g^{-1}g'g) = \varphi(g)^{-1}\varphi(g')\varphi(g) = \varphi(g').$$

Here we focus on the set S of transpositions in S_n. We argue by analysis–synthesis with a given homomorphism $\varphi : S_n \to (\mathbb{C}^*, \times)$. First note that **transpositions generate** S_n. Indeed cycles generate S_n (every permutation is a product of cycles), and every p-cycle $\tau = (x_1 \dots x_p)$ can be written as

$$\tau = (x_1\ x_2) \cdots (x_{p-1}\ x_p)(x_p\ x_1),$$

so every cycle, hence every permutation, is a product of transpositions.

Also, **transpositions (and more generally cycles of the same length) are conjugate in** S_n. If $\tau = (x_1 \dots x_p)$ and $\sigma \in S_n$, then

$$\sigma \circ (x_1 \dots x_p) \circ \sigma^{-1} = (\sigma(x_1) \dots \sigma(x_p)).$$

Thus any two p-cycles are conjugate via a σ sending $x_i \mapsto y_i$.
Now transpositions are conjugate and they generate S_n. If τ is a transposition (exists when $n \geq 2$), it has order 2, hence

$$\varphi(\tau)^2 = \varphi(\tau^2) = \varphi(id) = 1,$$

so $\varphi(\tau) \in \{\pm 1\}$. Since φ is constant on transpositions, either it is 1 on all of them (the trivial homomorphism), or it is -1 on all transpositions, which is the sign homomorphism (it agrees with the sign on generators).

Thus, for $n \geq 2$, **the homomorphisms** $S_n \to \mathbb{C}^*$ **are precisely the trivial character and the sign**. In representation-theoretic language: the *degree-1 characters* of S_n are the trivial character and the sign.

Solution to Exercise 3:

To show $(1, k)$ generate S_n, it suffices to express any transposition as a product of them. For a transposition (i, j) with $i \neq j$ and $i, j \neq 1$ (otherwise it already is of the form $(1, k)$), note

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

Hence **the transpositions** $(1, k)$ **for** $2 \leq k \leq n$ **generate** S_n.

Since $(1, k)$ generate S_n, to show adjacent transpositions $(k, k+1)$ (for $1 \leq k \leq n-1$) generate it, it suffices to write each $(1, k)$ as a product of adjacent transpositions. For $3 \leq k \leq n$, by cycle conjugation,

$$(k-1, k)(1, k-1)(k-1, k)^{-1} = (1, k).$$

If $k = 3$ we're done; otherwise iterate. Since the property holds for $k = 2$, induction shows every $(1, k)$ is a product of adjacent transpositions; thus **the adjacent transpositions generate** S_n.

To show $\tau = (1,2)$ and $\gamma = (1,2,\ldots,n)$ generate S_n, it suffices to produce each adjacent transposition $(k,k+1)$ from them. We already have $\tau = (1,2)$. Moreover, for $1 \leq k \leq n-2$,

$$\gamma \circ (k,k+1) \circ \gamma^{-1} = (k+1,k+2),$$

so

$$(k,k+1) = \gamma^{k-1} \circ (1,2) \circ (\gamma^{k-1})^{-1}.$$

Therefore $(1,2)$ **and** $(1,2,\ldots,n)$ **generate** S_n.

Minimal number of transpositions needed: the first two examples show $n-1$ suffice. We now show one cannot do better. If you remove one $(1,k)$, say $(1,j)$, then all remaining $(1,k)$ with $k \neq j$ fix j. If they still generated S_n, every permutation would fix j, which is false for $n \geq 3$ (e.g. $(1,j')$ with $j' \neq j$).
More generally, consider transpositions $\tau_1,\ldots,\tau_l$. If there exist i,j such that, using only τ_k, starting from i you can never reach j (i.e. for every word in the τ_k the image of i is never j), then any permutation sending i to j (e.g. (i,j)) is not a product of the τ_k. So a necessary condition for a set of transpositions to generate S_n is that from any vertex you can reach any other using those transpositions; in graph terms, the graph with vertices $\{1,\ldots,n\}$ and edges $\{i,j\}$ whenever (i,j) is one of the τ_k must be **connected**.

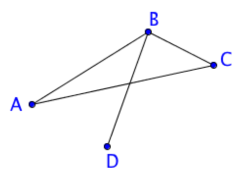

Figure 1: Connected graph

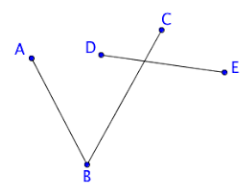

Figure 2: Disconnected graph

We show by induction on $n \geq 2$ that any connected graph with n vertices has at least $n-1$ edges.
Clear for $n = 2$.
Assume true for n. Let G be a graph on $n+1$ vertices. Let A be the number of edges, S the set of vertices, and $\delta(x)$ the degree of $x \in S$. Then

$$\sum_{x \in S} \delta(x) = 2A.$$

If $\delta(x) \geq 2$ for all x, then $A \geq n+1$ immediately.
Otherwise there exists a vertex of degree 1; remove it and its incident edge to get a graph G' with n vertices and $A-1$ edges. By induction $A-1 \geq n$, hence $A \geq n+1$.
Thus a connected n-vertex graph has at least $n-1$ edges; therefore **at least** $n-1$ **transpositions are needed** to generate S_n.

Solution to Exercise 4:

The general idea also applies to showing reflections generate $O(E)$ for a Euclidean space E: we **fix points step by step**. Given $\sigma \neq id$, compose with a well-chosen transposition τ that fixes one more point, then apply the induction hypothesis to $\tau\sigma$, write $\tau\sigma$ as a product of transpositions, and finally move τ to the other side using $\tau^2 = id$.
We prove by induction for $n \geq 2$:
For any set E with $|E| = n$ and any permutation σ of E, σ is a product of transpositions.
If $|E| = 2$, say $E = \{x_1, x_2\}$, then $S(E) = \{id, (x_1, x_2)\}$ and the claim holds (by convention id is an empty product of transpositions).
Assume true for n. Let $|E| = n + 1$ and $\sigma \in S(E)$.
If $\sigma = id$, nothing to do.
Otherwise there exists $x \in E$ with $\sigma(x) \neq x$. Set $y = \sigma(x)$ and let $\tau = (x, y)$ so that $\tau\sigma(x) = x$ and $\tau\sigma$ induces a permutation on $E \setminus \{x\}$, which has cardinality at least 2. By induction there are transpositions $\tau_1, \ldots, \tau_l$ with $\tau\sigma = \prod_{k=1}^{l} \tau_k$. Multiplying by τ gives $\sigma = \tau \prod_{k=1}^{l} \tau_k$, since $\tau^2 = id$.
Hence by induction **if $|E| \geq 2$, transpositions generate $S(E)$**.

Solution to Exercise 5:

This is quite abrupt and uses facts about $\mathscr{A}_n$. Generally, to show a group G is simple, take a nontrivial normal subgroup H and show that H **contains some conjugacy-stable subset that generates** G. Being normal, H is closed under conjugation, hence contains the whole subset; being a group, it is closed under products; if that subset generates G, then $H = G$. For instance, one can show $SO_3(\mathbb{R})$ is simple using that it is generated by rotations by π around axes ("half-turns").
Here the good subset will be 3-cycles. We will show: **3-cycles generate $\mathscr{A}_n$**, and **for $n \geq 5$, any two 3-cycles are conjugate $\underline{\text{in } \mathscr{A}_n}$**.

3-cycles generate $\mathscr{A}_n$: an element of $\mathscr{A}_n$ has sign $+1$. Since transpositions have sign -1 and any permutation is a product of transpositions, elements of $\mathscr{A}_n$ are exactly the products of an even number of transpositions. It suffices to show a product of two transpositions is a product of 3-cycles. Let (i, j) and (k, l) be transpositions.
If they are equal, the product is id, an empty product of 3-cycles.
If they share one element, say $j = k$, then $(i, j)(k, l) = (i, j, l)$, a 3-cycle.
Otherwise, note $(i, j)(k, l) = (i, l, k)(i, j, k)$ (check by expansion).
Hence **3-cycles generate $\mathscr{A}_n$**.

Now show that for $n \geq 5$, any two 3-cycles are conjugate $\underline{\text{within } \mathscr{A}_n}$. Let (i, j, k) and (i', j', k') be 3-cycles. Choose $\sigma \in S_n$ with $\sigma(i) = i'$, $\sigma(j) = j'$, $\sigma(k) = k'$. Then $\sigma \circ (i, j, k) \circ \sigma^{-1} = (i', j', k')$.
If σ is even, we are done.

Otherwise, take two elements $p, q \in \{1, \dots, n\} \setminus \{i, j, k\}$ (possible since $n \geq 5$) and replace σ by $\tau\sigma$ with $\tau = (p, q)$. The equality remains true and $\tau\sigma$ is even. Thus **for $n \geq 5$, any two 3-cycles are conjugate in $\mathscr{A}_n$.**

For simplicity: let $H \lhd \mathscr{A}_n$ with $H \neq \{id\}$. As above, it suffices to show H contains a 3-cycle, after which $H = \mathscr{A}_n$. Pick $\sigma \in H \setminus \{id\}$ maximizing the number N of fixed points among elements of $H \setminus \{id\}$. We will show σ is a 3-cycle by contradiction, by inspecting its disjoint cycle decomposition and constructing, via a suitable 3-cycle (to stay in $\mathscr{A}_n$), an element of H with strictly more fixed points.

If the decomposition consists only of transpositions, then there are at least two (since σ is even). WLOG let them be $(1, 2)$ and $(3, 4)$, so $\sigma = (1, 2)(3, 4)\tau_1 \cdots \tau_r$ where each τ_i has support disjoint from $\{1, 2, 3, 4\}$. Let $\gamma = (3, 4, 5)$ (possible since $n \geq 5$). Then by conjugation of cycles,

$$\gamma \circ \sigma \circ \gamma^{-1} = (\gamma \circ (1, 2) \circ \gamma^{-1})(\gamma \circ (3, 4) \circ \gamma^{-1})(\gamma \circ \tau_1 \circ \gamma^{-1}) \cdots = (1, 2)(4, 5)\tau_1' \cdots \tau_r'.$$

Set $\rho = \gamma \circ \sigma \circ \gamma^{-1} \circ \sigma^{-1}$. One checks $\rho(1) = 1$ and $\rho(2) = 2$. Any fixed point $i > 5$ of σ is also fixed by ρ. Since $1, 2, 3, 4$ are not fixed by σ, all N fixed points lie in $\{5, \dots, n\}$. If 5 is not fixed by σ, then *all* fixed points of σ remain fixed by ρ, and $1, 2$ are also fixed, so ρ has at least $N + 2$ fixed points. Otherwise ρ has at least $N + 1$ fixed points. Also $\rho \neq id$ (the conjugate is not equal to σ). But $\gamma \circ \sigma \circ \gamma^{-1} \in H$ (normality) and hence $\rho \in H$, contradicting maximality of N.

Thus at least one cycle in the decomposition is not a transposition; WLOG it is $(1, 2, 3, \dots)$. Suppose σ is not a 3-cycle. We repeat the idea by finding two further points not fixed by σ (they were $4, 5$ above). If there is another cycle, we can choose two points not fixed. If σ is a single even cycle of length ≥ 5, again there are two such points. Relabel so they are $4, 5$. Again set $\gamma = (3, 4, 5)$. Writing $\sigma = c_1 \cdots c_r$ with $c_1 = (1, 2, 3, \dots)$, we have

$$\gamma \circ \sigma \circ \gamma^{-1} = (\gamma \circ c_1 \circ \gamma^{-1})(\gamma \circ c_2 \circ \gamma^{-1}) \cdots = (1, 2, 4, \dots)c_2' \cdots c_r'.$$

Set $\rho = \gamma \circ \sigma \circ \gamma^{-1} \circ \sigma^{-1}$. As before, $\rho \in H$, $\rho \neq id$, $\rho(2) = 2$, and every fixed point > 5 of σ is fixed by ρ. Since σ does not fix $1, 2, 3, 4, 5$, ρ has at least $N+1$ fixed points—contradiction.

Therefore σ is a 3-cycle; from the preliminary remarks it follows $H = \mathscr{A}_n$ and **$\mathscr{A}_n$ is simple for $n \geq 5$.**

A remark: for a group G, the *derived group* $D(G)$ is generated by commutators $[g, g'] = gg'g^{-1}g'^{-1}$. It is always normal and $G/D(G)$ is abelian (the abelianization). A corollary of the above is that **for $n \geq 5$, the derived subgroup of S_n is $\mathscr{A}_n$.**

Solution to Exercise 6:

Define

$$\begin{aligned}\varphi\,:\,G &\to S(G)\\ g &\mapsto \varphi(g)\end{aligned}$$

where

$$\begin{aligned}\varphi(g)\,:\,G &\to G\\ h &\mapsto gh.\end{aligned}$$

It is a homomorphism (the left translation action).
Each $\varphi(g)$ is a bijection with inverse $\varphi(g^{-1})$. For all $g, g', h \in G$,

$$\varphi(gg')(h) = gg'h = \varphi(g)(\varphi(g')(h)),$$

so $\varphi(gg') = \varphi(g) \circ \varphi(g')$.
Injectivity: if $g \in \ker\varphi$, then $\varphi(g) = id$, so $gh = h$ for all h, hence $g = e_G$.
Thus $\mathrm{Im}(\varphi) \leq S(G)$ and $G \simeq \mathrm{Im}(\varphi) \subset S(G)$: **Cayley's theorem**.

In particular, if $|G| = n < \infty$, then G is isomorphic to a subgroup of S_n.

Solution to Exercise 7:

Let $H \leq S_n$ be of index $2 \leq r \leq n-1$ ($n \geq 5$). Inspired by Cayley's proof, define

$$\begin{aligned}\varphi\,:\,S_n &\to S(S_n/H)\\ \sigma &\mapsto \varphi(\sigma)\end{aligned}$$

where

$$\begin{aligned}\varphi(\sigma)\,:\,S_n/H &\to S_n/H\\ \tau H &\mapsto \sigma\tau H.\end{aligned}$$

This is the action by left translation.
$\varphi(\sigma)$ is a bijection: injectivity follows since $\sigma\tau H = \sigma\tau' H \Rightarrow \tau H = \tau' H$; surjectivity since $\tau H = \varphi(\sigma)(\sigma^{-1}\tau H)$.
As in Exercise 6, φ is a homomorphism. Its kernel is normal in S_n: in general, for any homomorphism $\psi : G \to G'$, $\ker\psi \lhd G$ (since $\psi(hgh^{-1}) = \psi(h)\psi(g)\psi(h)^{-1} = e$ whenever $g \in \ker\psi$).

We now use the suggested fact (relying on the simplicity of $\mathscr{A}_n$ for $n \geq 5$): **when $n \geq 5$, the only normal subgroups of S_n are S_n, $\mathscr{A}_n$ and $\{id\}$.** Indeed, if $G \lhd S_n$, then $G \cap \mathscr{A}_n \lhd \mathscr{A}_n$ which is simple, hence $G \cap \mathscr{A}_n$ is either $\mathscr{A}_n$ or $\{id\}$. If $G \cap \mathscr{A}_n = \mathscr{A}_n$, then $\mathscr{A}_n \leq G$, and by Lagrange $|\mathscr{A}_n| = \frac{n!}{2}$ divides $|G|$ and $|G|$ divides $n!$, so $|G| \in \{\frac{n!}{2}, n!\}$, i.e. $G \in \{\mathscr{A}_n, S_n\}$. If $G \cap \mathscr{A}_n = \{id\}$, one checks $G = \{id\}$ (otherwise odd elements multiply to give an even nontrivial element in the intersection).

Thus $\ker\varphi$ is S_n or $\{id\}$ or $\mathscr{A}_n$. It cannot be $\{id\}$ because $|S_n| = n! > |S(S_n/H)| = r!$ (so φ is not injective). Also, if $\sigma \in \ker\varphi$, then for all τ, $\sigma\tau H = \tau H$, so taking $\tau = \sigma^{-1}$ gives $\sigma \in H$, hence $\ker\varphi \subset H$. Since $[S_n : H] \geq 2$, $\ker\varphi \neq S_n$, so $\ker\varphi = \mathscr{A}_n \subset H$. By Lagrange,

$$|\mathscr{A}_n| = \frac{n!}{2} \mid |H| = \frac{n!}{r} \quad \Rightarrow \quad r \leq 2,$$

hence $r = 2$ and $H = \mathscr{A}_n$.

If $[S_n : H] = n$, then $|H| = (n-1)!$. Now $\ker\varphi \subset H$ cannot be S_n nor $\mathscr{A}_n$ (else $\frac{n!}{2}$ would divide $(n-1)!$), so φ is injective and $\varphi(H) \leq S(S_n/H)$ with $\varphi(H) \simeq H$. Note that elements of $\varphi(H)$ fix $H \in S_n/H$ (and conversely), so each $\varphi(\sigma)$ is determined by the induced permutation $\widetilde{\varphi(\sigma)}$ on $S_n/H \setminus \{H\}$, giving an isomorphism $\varphi(H) \simeq S(S_n/H \setminus \{H\}) \simeq S_{n-1}$. Hence

$$H \simeq \varphi(H) \simeq S_{n-1}.$$

<u>Solution to Exercise 8:</u>

Useful remark: **if $\varphi : G \to G'$ is a homomorphism and $g \in G$ has finite order n, then $\varphi(g)$ has order dividing** n, since $\varphi(g)^n = \varphi(g^n) = e$. This is particularly useful for $S_n \to S_n$: images of elements of small/prime order (transpositions, order 2; 3-cycles, order 3) can only have restricted orders.

Let $\varphi \in \mathrm{Aut}(S_n)$. Since $\mathscr{A}_n$ **is generated by 3-cycles** (Exercise 5), to see that φ stabilizes $\mathscr{A}_n$ it suffices that images of 3-cycles lie in $\mathscr{A}_n$. If γ is a 3-cycle, its order is 3, so $\varphi(\gamma)$ has order dividing 3 but is not id (injectivity), hence has order 3. Since **the order of a permutation is the lcm of its cycle lengths**, all cycles in $\varphi(\gamma)$ have length 3, so $\varphi(\gamma) \in \mathscr{A}_n$.
Therefore every automorphism of S_n stabilizes $\mathscr{A}_n$.

<u>Solution to Exercise 9:</u>

<u>Question 1:</u> For $\sigma \in S_n$, $Z(\sigma)$ is a subgroup: clearly $id \in Z(\sigma)$; if $\tau, \tau' \in Z(\sigma)$ then $\tau \circ \tau' \in Z(\sigma)$; and if $\tau \in Z(\sigma)$ then $\tau^{-1} \in Z(\sigma)$.
If $\varphi \in \mathrm{Aut}(S_n)$ and $\tau \in \varphi(Z(\sigma))$, say $\tau = \varphi(\tau')$ with $\tau' \in Z(\sigma)$, then

$$\tau \circ \varphi(\sigma) = \varphi(\tau') \circ \varphi(\sigma) = \varphi(\tau' \circ \sigma) = \varphi(\sigma \circ \tau') = \varphi(\sigma) \circ \varphi(\tau') = \varphi(\sigma) \circ \tau,$$

so $\tau \in Z(\varphi(\sigma))$, hence $\varphi(Z(\sigma)) \subset Z(\varphi(\sigma))$. Applying the same to φ^{-1} gives equality.

Question 2: Suppose $\sigma = \tau_1 \cdots \tau_k$ where the τ_i are disjoint transpositions. Writing $\tau_i = (x_1^{(i)}, x_2^{(i)})$, conjugation yields

$$\gamma \circ \sigma \circ \gamma^{-1} = (\gamma(x_1^{(1)}), \gamma(x_2^{(1)})) \cdots (\gamma(x_1^{(k)}), \gamma(x_2^{(k)})).$$

Thus $\gamma \in Z(\sigma)$ iff $\{\tau_1, \dots, \tau_k\} = \{(\gamma(x_1^{(i)}), \gamma(x_2^{(i)}))\}_i$. There are $(n-2k)!$ ways to permute the other $n-2k$ points, $k!$ ways to match the k 2-cycles, and for each matched pair two ways to align the two points. Hence

$$|Z(\sigma)| = 2^k\, k!\, (n-2k)!.$$

Question 3: Let τ be a transposition and write $\varphi(\tau)$ as a product of k transpositions. By Question 1, $Z(\varphi(\tau)) = \varphi(Z(\tau))$, so $|Z(\varphi(\tau))| = |Z(\tau)| = 2(n-2)!$. Using Question 2,

$$2^k k!(n-2k)! = 2(n-2)! \quad \Longrightarrow \quad 2^{k-1}k! = (n-2)(n-3)\cdots(n-2k+1).$$

If $k = 2$, this gives $(n-2)(n-3) = 4$, impossible in $\mathbb{N}$ because the LHS is odd. If $k \geq 3$, one shows the RHS has an odd factor unless $k = 3$ and $n = 6$, which is excluded. Hence $k = 1$ and $\varphi(\tau)$ is a transposition.

Question 4: To show φ is inner, find σ with $\forall u$, $\varphi(u) = \sigma \circ u \circ \sigma^{-1}$. A homomorphism from S_n is determined by the images of $(1,k)$, $2 \leq k \leq n$ (they generate S_n). It suffices that σ agrees with φ on these.
Consider the images of $(1,k)$. They are transpositions by Question 3. Let $(x_1, x_2) = \varphi((1,2))$ and $(y_1, y_2) = \varphi((1,3))$. These two do not commute (since $(1,2)$ and $(1,3)$ don't), so their supports intersect; WLOG $y_1 = x_1$ and write $y_2 = x_3$. We claim: there exist pairwise distinct $x_1, \dots, x_n$ such that for all $k \in \{2, \dots, n\}$, $\varphi((1,k)) = (x_1, x_k)$. Define the property $P(i)$: there exist distinct $x_1, \dots, x_i$ with $\varphi((1,k)) = (x_1, x_k)$ for $2 \leq k \leq i$. $P(2)$ and $P(3)$ hold. Suppose $P(i-1)$ holds for $i > 3$. Since $(1,i)$ commutes with none of $(1,k)$, $2 \leq k \leq i-1$, the support of $\varphi((1,i))$ meets each (x_1, x_k). If x_1 were not in its support, then all x_k would be, which is impossible unless $i = 4$, in which case $\varphi((1,4)) = (x_2, x_3)$. But

$$(x_2, x_3) = (x_1, x_3)(x_1, x_2)(x_1, x_3) = \varphi((1,3))\varphi((1,2))\varphi((1,3)) = \varphi((1,3)(1,2)(1,3)),$$

so injectivity would force $(1,4) = (1,3)(1,2)(1,3)$, contradiction. Hence x_1 is in the support; name the other element x_i and $P(i)$ holds.
Define σ by $\sigma(i) = x_i$. The conjugation formula gives $\sigma \circ (1,k) \circ \sigma^{-1} = (x_1, x_k) = \varphi((1,k))$ for $2 \leq k \leq n$, hence $\varphi(u) = \sigma \circ u \circ \sigma^{-1}$ for all u. Thus **if $n \neq 6$, every automorphism of S_n is inner**.

Solution to Exercise 10:

Show there is no injective homomorphism $S_2 \to \mathscr{A}_3$. For injective $\varphi : G \to G'$ between finite groups, $\mathrm{Im}(\varphi)$ is a subgroup of G' and $|G| = |\mathrm{Im}(\varphi)|$ divides $|G'|$ (Lagrange). Also the target must have a subgroup of order $|G|$. Since $2 \nmid |\mathscr{A}_3| = 3$, no injective $S_2 \to \mathscr{A}_3$ exists.

For $n = 3$, we show $\mathscr{A}_4$ has no subgroup of order $6 = |S_3|$. More generally: **if** $|G| = 2n$ **and** $H \leq G$ **has** $|H| = n$**, then** $g^2 \in H$ **for all** $g \in G$. Indeed, $[G : H] = 2$ so $G = H \cup gH$ for any $g \notin H$. If $g^2 \in gH$, then $g^2 = gh$ for some $h \in H$, hence $g = h \in H$, contradiction; thus $g^2 \in H$. In $\mathscr{A}_4$, $|\mathscr{A}_4| = 12 = 2 \times 6$; if H had order 6, then H would contain all squares of elements of $\mathscr{A}_4$. But any 3-cycle τ satisfies $\tau = (\tau^{-1})^2$, so H contains all eight 3-cycles—impossible. Hence no injective $S_3 \to \mathscr{A}_4$.

For general $n \geq 4$: a necessary condition is $|S_n| = n!$ divides $|\mathscr{A}_{n+1}| = \frac{(n+1)!}{2}$, which forces n odd (say $n = 2k + 1$). Suppose by contradiction there is an injective $\varphi : S_{2k+1} \hookrightarrow \mathscr{A}_{2k+2}$. Consider

$$\begin{aligned} \psi : \mathscr{A}_{2k+2} &\to S(\mathscr{A}_{2k+2}/\mathrm{Im}(\varphi)) \\ \sigma &\mapsto (\tau \,\mathrm{Im}(\varphi) \mapsto \sigma\tau \,\mathrm{Im}(\varphi)). \end{aligned}$$

As in Exercise 7, ψ is a homomorphism. Its kernel is normal in $\mathscr{A}_{2k+2}$; for $n \geq 5$, $\mathscr{A}_{2k+2}$ is simple, so $\ker \psi$ is $\{id\}$ or $\mathscr{A}_{2k+2}$. But

$$|S(\mathscr{A}_{2k+2}/\mathrm{Im}(\varphi))| = \left(\frac{(2k+2)!}{2(2k+1)!}\right)! = (k+1)!,$$

while $|\mathscr{A}_{2k+2}| = \frac{(2k+2)!}{2} = (k+1)(2k+1)! > (k+1)!$, so ψ is not injective; hence $\ker \psi = \mathscr{A}_{2k+2}$. As in Exercise 7, this implies $\mathscr{A}_{2k+2} \subset \mathrm{Im}(\varphi)$, so $|\mathrm{Im}(\varphi)| = |\mathscr{A}_{2k+2}|$, contradiction since $|(2k+1)!| < |\mathscr{A}_{2k+2}|$.

Therefore, **there is no injective group homomorphism** $S_n \hookrightarrow \mathscr{A}_{n+1}$ **for** $n \geq 2$.