7. Permutation Groups

Recall that the set of all permutations of $\{1, \dots, n\}$ under composition is a group of oder $n!$, denoted by S_n, which is called the **symmetric group** or **permutation group** of degree n. Permutations are usually denoted by Greek letters like π, ρ, and σ.

The following theorem indicates that permutation groups and their subgroups play a key-role in the investigation of finite groups.

Theorem 7.1. If G is a finite group of order n, then G is isomorphic to a subgroup of S_n.

Proof. Let $G = \{a_1, \dots, a_n\}$ and let

$$\begin{array}{rccc} \varphi: & G & \to & S_n \\ & x & \mapsto & \pi_x \end{array}$$

where for $i \in \{1, \dots, n\}$, $\pi_x(i)$ is such that $xa_i = a_{\pi_x(i)}$.

φ is well-defined: We have to show that for all $x \in G$, $\varphi(x) \in S_n$. Let $x \in G$, then for all $i, j \in \{1, \dots, n\}$ we have

$$\pi_x(i) = \pi_x(j) \iff xa_i = xa_j \iff a_i = a_j \iff i = j\,.$$

Thus, for each $x \in G$, $\varphi(x) = \pi_x$ is an injective mapping from $\{1, \dots, n\}$ into $\{1, \dots, n\}$, which implies – since $\{1, \dots, n\}$ is a finite set – that $\varphi(x)$ is a permutation of $\{1, \dots, n\}$, or equivalently, $\varphi(x) \in S_n$.

φ is injective: If $\varphi(x) = \varphi(y)$, then for each $i \in \{1, \dots, n\}$ we have $\pi_x(i) = \pi_y(i)$, thus

$$xa_i = a_{\pi_x(i)} = a_{\pi_y(i)} = ya_i\,,$$

which implies $x = y$.

φ is a homomorphism: We have to show that $\varphi(xy) = \varphi(x)\,\varphi(y)$. For $x, y \in G$ and for any $i \in \{1, \dots, n\}$ we have

$$a_{\pi_{xy}(i)} = (xy)a_i = x(ya_i) = xa_{\pi_y(i)} = a_{\pi_x(\pi_y(i))}\,.$$

Thus, $\pi_{xy}(i) = \pi_x\big(\pi_y(i)\big)$ (for all $i \in \{1, \dots, n\}$), and hence, $\varphi(xy) = \varphi(x)\,\varphi(y)$.

By Corollary 6.2 and since φ is injective, G is isomorphic to a subgroup of S_n, namely to the image of φ. ⊣

It is common to write a permutation $\pi \in S_n$ in *two-row* notation, in which the top row of the $2 \times n$ matrix contains the integers $1, \dots, n$ and the effect of π on the integer i is written under i:

$$\pi = \begin{pmatrix} 1 & 2 & \dots & i & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(i) & \dots & \pi(n) \end{pmatrix}$$

In particular, the identity permutation is

$$\begin{pmatrix} 1 & 2 & \dots & i & \dots & n \\ 1 & 2 & \dots & i & \dots & n \end{pmatrix}$$

and is denoted by ι. For any permutation π and any integer k we set $\pi^0 := \iota$ and $\pi^{k+1} := \pi(\pi^k)$.

A more compact notation is the so-called *cycle notation*, which avoids repeating the same first row in each permutation. The theoretical basis for this notation is in the following result.

PROPOSITION 7.2. Let $\pi \in S_n$, $i \in \{1, \ldots, n\}$, and let k be the smallest positive integer for which $\pi^k(i)$ is in the set $\{i, \pi(i), \pi^2(i), \ldots, \pi^{k-1}(i)\}$. Then $\pi^k(i) = i$.

Proof. If $\pi^k(i) = \pi^r(i)$ for some non-negative $r < k-1$, then, for $k' = k - r$ we have $k \geq k' > 0$ and $\pi^{k'} = \iota$, which implies $\pi^{k'}(i) = i \in \{i, \pi(i), \ldots, \pi^{k-1}(i)\}$, and therefore, by our assumption, $k' = k$. ⊣

DEFINITION. A permutation $\rho \in S_n$ is a ***k*-cycle** if there exists a positive integer k and an integer $i \in \{1, \ldots, n\}$ such that

(1) k is the smallest positive integer such that $\rho^k(i) = i$, and
(2) ρ fixes each $j \in \{1, \ldots, n\} \setminus \{i, \rho(i), \ldots, \rho^{k-1}(i)\}$.

The k-cycle ρ is usually denoted $(i, \rho(i), \ldots, \rho^{k-1}(i))$.

For example the five non-identity elements of S_3 are all cycles, and may be written as

$$(1,2,3),\ (3,2,1),\ (1,2),\ (1,3),\ \textit{and}\ (2,3)\,.$$

Notice that for example $(1,2,3) = (2,3,1) = (3,1,2)$ and that not every permutation is a cycle, *e.g.*,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

is not a cycle.

DEFINITION. Two permutations ρ and σ are **disjoint** if each number moved by ρ is fixed by σ, or equivalently, each number moved by σ is fixed by ρ.

It is quite easy to see that disjoint permutations commute.

FACT 7.3. Let σ and ρ be disjoint permutations, then $\sigma\rho = \rho\sigma$, and in general, for all positive integers k, $(\sigma\rho)^k = \sigma^k\rho^k$.

Proof. Since σ and ρ are disjoint permutations, each number moved by σ is fixed by ρ and vice versa. So, the set of numbers moved by σ is disjoint from the set of numbers moved by ρ, and therefore it does not matter which permutation we carry out first. Consequently we get $(\sigma\rho)^k = \sigma^k\rho^k$ (for all positive integers k). ⊣

The next result shows that cycles are the "atoms" of permutations.

PROPOSITION 7.4. Every permutation $\pi \in S_n$ may be written as a product of disjoint cycles.

Proof. Let $\pi \in S_n$. By Proposition 7.2 and since the set $\{1, \ldots, n\}$ is finite, for every $i \in \{1, \ldots, n\}$ there is a positive integer k_i such that $\pi^{k_i}(i) = i$ and $\rho_i = (i, \pi(i), \ldots, \pi^{k_i-1}(i))$ is a k_i-cycle. We proceed by induction. Let $i_1 := 1$ and for $j \geq 1$ with $\sum_{\ell=1}^{j} k_{i_\ell} < n$ let i_{j+1} be the least number of the non-empty set

$$\{1, \ldots, n\} \setminus \bigcup \{\pi^k(i_\ell) : k \in \mathbb{Z} \textit{ and } 1 \leq \ell \leq j\}\,.$$

Further, let m be the least positive integer such that $\sum_{\ell=1}^{m} k_{i_\ell} = n$, then, by construction, $\pi = \rho_{i_1}\,\rho_{i_2}\,\ldots\,\rho_{i_m}$ and the ρ's are disjoint cycles. ⊣

DEFINITION. A decomposition of a permutation π into disjoint cycles is called a **cycle decomposition** of π.

For example the cycle decomposition of the permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 2 & 5 & 3 & 4 & 1 & 7 & 9 & 8 \end{pmatrix}$$

is $(1,6)(2)(3,5,4)(7)(8,9)$. It is usual to omit cycles of length 1, those integers fixed by π, and so π is abbreviated to $(1,6)(3,5,4)(8,9)$.

PROPOSITION 7.5. If ρ is a k-cycle, then $\operatorname{ord}(\rho) = k$, and consequently, if π is a product of disjoint cycles of length $k_1, \dots, k_r$, then $\operatorname{ord}(\pi) = \operatorname{lcm}(k_1, \dots, k_r)$, where $\operatorname{lcm}(k_1, \dots, k_r)$ is the lowest common multiple of the integers $k_1, \dots, k_r$.

Proof. If ρ is a k-cycle, then there is an $i \in \{1, \dots, n\}$ such that $\rho = \big(i, \rho(i), \dots, \rho^{k-1}(i)\big)$ where $\rho^k(i) = i$. Hence, for every non-negative $\ell < k$ we have $\rho^k\big(\rho^\ell(i)\big) = \rho^\ell\big(\rho^k(i)\big) = \rho^\ell(i)$, which shows that $\rho^k = \iota$, thus $\operatorname{ord}(\rho) \geq k$. On the other hand, by definition of k, $\rho^\ell \neq \iota$ for any positive $\ell < k$, thus, $\operatorname{ord}(\rho) = k$.

Let π be a product of disjoint cycles $\rho_1, \dots, \rho_r$ of length $k_1, \dots, k_r$ and let $\operatorname{ord}(\pi) = k$. By Fact 7.3 we have $\iota = \pi^k = \rho_1^k \, \dots \, \rho_r^k$ which implies that for every $1 \leq j \leq r$, k_j divides k, thus, $\operatorname{ord}(\pi) \geq \operatorname{lcm}(k_1, \dots, k_r)$. On the other hand, it is easy to see that for $k = \operatorname{lcm}(k_1, \dots, k_r)$, $\pi^k = \iota$, thus, $\operatorname{ord}(\pi) = k$. ⊣

For example, the order of $(1,2,3,4)(5,6,7)(8,9)$ is equal to $\operatorname{lcm}(4,3,2) = 12$. However, the permutation $(1,2,3,4)(2,6,7)(3,9)$ is not a product of disjoint cycles (and so need not have order 12). In fact,

$$(1,2,3,4)(2,6,7)(3,9) = (1,2,6,7,3,9,4)\,,$$

and therefore has order 7.

The following result shows that for any permutations π and ρ, π has the same cycle structure as $\rho\pi\rho^{-1}$.

PROPOSITION 7.6. Let π and ρ be permutations in S_n. The cycle decomposition of the permutation $\rho\pi\rho^{-1}$ is obtained from that of π by replacing each integer i in the cycle decomposition of π with the integer $\rho(i)$.

Proof. Consider the effect that $\rho\pi\rho^{-1}$ has on the integer $\rho(i)$:

$$\rho\pi\rho^{-1}\big(\rho(i)\big) = \rho\big(\pi(i)\big)\,,$$

or in other words, $\rho\pi\rho^{-1}$ maps $\rho(i)$ to $\rho\big(\pi(i)\big)$. Hence, in the cycle decomposition of $\rho\pi\rho^{-1}$, the number $\rho(i)$ stands to the left of $\rho\big(\pi(i)\big)$, so

$$\rho\pi\rho^{-1} = \dots \big(\dots \rho(i), \rho\big(\pi(i)\big) \dots \big) \dots\,,$$

whereas in the cycle decomposition of π, i stands to the left of $\pi(i)$, so

$$\pi = \dots \big(\dots i, \pi(i) \dots \big) \dots\,,$$

which completes the proof. ⊣

Definition. A **transposition** is a cycle of length 2, and an **elementary transposition** is a transposition of the form $(i, i+1)$.

Lemma 7.7. Every k-cycle can be written as a product of $k-1$ transpositions and every transposition can be written as product of an odd number of elementary transpositions.

Proof. It is easily verified that

$$(i_1, i_2, \dots, i_k) = (i_1, i_2)(i_2, i_3)\dots(i_{k-1}, i_k)\,,$$

thus, every k-cycle can be written as a product of $k-1$ transpositions. Further, let j be a positive integer and let $(i, i+j)$ be a transposition. If $j = 1$, then $(i, i+1)$ is an elementary transposition and we are done. Otherwise, it is easy to see that

$$(i, i+j) = \underbrace{(i, i+1)\dots(i+j-1, i+j)}_{j \text{ elementary transpositions}}\,\underbrace{(i+j-2, i+j-1)\dots(i, i+1)}_{j-1 \text{ elementary transpositions}}\,,$$

thus, $(i, i+j)$ is the product of $2j-1$ elementary transpositions and $2j-1$ is always odd. ⊣

Proposition 7.8.

(1) Each permutation can be written as a product of (elementary) transpositions.
(2) S_n is generated by the transpositions $(1,2)$, $(1,3), \dots, (1,n)$.
(3) S_n is generated by the two permutations $(1,2)$ and $(1,2,\dots,n)$.

Proof. (1) follows from Proposition 7.4 and Lemma 7.7.

(2) By (1), it is enough to show that every transposition (i,j), where $i < j$, belongs to $\big\langle\big\{(1,2),\ (1,3), \dots, (1,n)\big\}\big\rangle$. Now, if $i = 1$, then we are done. Otherwise, it is easy to see that $(i,j) = (1,i)(1,j)(1,i)$.

(3) See Hw10.Q47. ⊣

The factorisation of a cycle into transpositions is not unique. Moreover, it is not even true that the number of transpositions in any factorisation of a given cycle is always the same, for example $(1,3) = (2,3)(1,2)(2,3)$. However, we will see that the numbers of transpositions in any two decompositions of a given permutation are either both even or both odd.

Definition. For any positive integer n, let Δ_n be the polynomial in n variables $x_1, \dots, x_n$ defined by

$$\Delta_n(x_1, \dots, x_n) = \prod_{1 \le i < j \le n} \big(x_i - x_j\big)\,,$$

and for any permutation $\pi \in S_n$ let $\pi \cdot \Delta_n$ be the polynomial

$$\prod_{1 \le i < j \le n} \big(x_{\pi(i)} - x_{\pi(j)}\big)\,.$$

The following properties are easily checked.

Fact 7.9.

(a) $\iota \cdot \Delta_n = \Delta_n$.
(b) $(\pi\rho) \cdot \Delta_n = \pi \cdot (\rho \cdot \Delta_n)$.
(c) For any real number λ, $\pi \cdot (\lambda\Delta_n) = \lambda(\pi \cdot \Delta_n)$.

Definition. For any $\pi \in S_n$, the polynomial Δ_n is either equal to $\pi \cdot \Delta_n$, in which case we say that the permutation π is **even**, or $\Delta_n = -\pi \cdot \Delta_n$, in which case we say that π is **odd**. We write $\operatorname{sgn}(\pi) = 1$ if π is even and $\operatorname{sgn}(\pi) = -1$ if π is odd, so that $\pi \cdot \Delta_n = \operatorname{sgn}(\pi)\,\Delta_n$.

Theorem 7.10. The map $\operatorname{sgn} : S_n \to C_2$ is a homomorphism.

Proof. We must show that $\operatorname{sgn}(\pi\rho) = \operatorname{sgn}(\pi)\operatorname{sgn}(\rho)$:

$$\begin{aligned}
\operatorname{sgn}(\pi\rho)\,\Delta_n &= (\pi\rho)\cdot\Delta_n && \text{by definition}\\
&= \pi\cdot(\rho\cdot\Delta_n) && \text{by Fact 7.9 (b)}\\
&= \pi\cdot\big(\operatorname{sgn}(\rho)\Delta_n\big) && \text{by definition}\\
&= \operatorname{sgn}(\rho)(\pi\cdot\Delta_n) && \text{by Fact 7.9 (c)}\\
&= \operatorname{sgn}(\rho)\operatorname{sgn}(\pi)\Delta_n && \text{by definition}
\end{aligned}$$

Thus, $\operatorname{sgn}(\pi\rho) = \operatorname{sgn}(\rho)\operatorname{sgn}(\pi) = \operatorname{sgn}(\pi)\operatorname{sgn}(\rho)$, as required. ⊣

Corollary 7.11. For any permutation $\pi \in S_n$, $\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi)$, and for any $\pi, \rho \in S_n$,

$$\operatorname{sgn}(\rho\pi\rho^{-1}) = \operatorname{sgn}(\pi)\,.$$

Proof. By Fact 7.9 and from the definition we have $\operatorname{sgn}(\iota) = 1$. Thus, by Theorem 7.10, we have

$$1 = \operatorname{sgn}(\iota) = \operatorname{sgn}(\pi\pi^{-1}) = \operatorname{sgn}(\pi)\operatorname{sgn}(\pi^{-1})\,,$$

which implis $\operatorname{sgn}(\pi) = \operatorname{sgn}(\pi^{-1})$.

Further, since

$$\operatorname{sgn}(\pi)\operatorname{sgn}(\rho) = \operatorname{sgn}(\rho)\operatorname{sgn}(\pi)\,,$$

by Theorem 7.10 it follows that

$$\operatorname{sgn}(\rho\pi\rho^{-1}) = \operatorname{sgn}(\rho)\operatorname{sgn}(\pi)\operatorname{sgn}(\rho^{-1}) = \operatorname{sgn}(\pi)\operatorname{sgn}(\rho)\operatorname{sgn}(\rho^{-1}) = \operatorname{sgn}(\pi)\,.$$

⊣

Corollary 7.12. All transpositions are odd, and a k-cycle is odd if and only if k is even.

Proof. Firstly notice that by the definition of sgn, every elementary transposition $(i, i+1)$ is odd. Indeed, we change the sign of just one factor of the polynomial Δ_n, namely of the factor $\big(x_i - x_{i+1}\big)$. Now, by Lemma 7.7, every transposition can be written as product of an odd number of elementary transpositions, and therefore, by Theorem 7.10, all transpositions are odd.

Again by Lemma 7.7, every k-cycle can be written as a product of $k-1$ transpositions, and therefore, by Theorem 7.10, a k-cycle is odd if and only if k is even. ⊣

As an immediate consequence of Corollary 7.12 we get

Corollary 7.13. A permutation is even (odd) if and only if it can be written as a product of an even (odd) number of transpositions. In particular, ι is even.

By the way, if $A = (a_{i,j})$ is an $n \times n$ matrix, then

$$\det(A) := \sum_{\pi \in S_n} \Big(\operatorname{sgn}(\pi) \prod_{i=1}^{n} a_{i,\pi(i)} \Big) .$$

Definition. The kernel of the homomorphism $\operatorname{sgn} : S_n \to C_2$ is the **alternating group** A_n. Or in other words,

$$A_n = \{\pi \in S_n : \ \pi \text{ is even}\} .$$

For example, $A_3 = \big\{\iota, (1,2,3), (3,2,1)\big\}$, and therefore, $A_3 \cong C_3$. But for $n \geq 4$, A_n is a non-abelian group of order $n!/2$. In particular, as we will see later, A_4 is isomorphic to the tetrahedron-group T and A_5 is isomorphic to the dodecahedron-group D, whereas the cube-group C is isomorphic to S_4.

By the First Isomorphism Theorem and the fact that for $n \geq 2$ the map sgn is surjective, for every $n \geq 2$, $A_n \trianglelefteq S_n$ and $|S_n : A_n| = 2$. This implies that for every $n \geq 3$, S_n is not simple. It is easy to see that A_3 is the only non-trivial normal subgroup of S_3 and that A_3 is simple (since it is isomorphic to C_3). On the other hand, the group S_4 has a normal subgroup of order 4 (*cf.* Hw10.Q50 (c)) which is also a normal subgroup of A_4, thus, A_4 is not the only non-trivial normal subgroup of S_4 and A_4 is not simple. But one can show that for every $n \geq 5$, A_n is simple and it is the only non-trivial normal subgroup of S_n (we omit the proof).

We have seen that S_n is generated by its transpositions and that all transpositions are odd. Thus, no transposition belongs to A_n. To find simple generators for A_n, we have to consider even permutations. The simplest even permutations, beside the identity, are 3-cycles, and indeed:

Proposition 7.14. The alternating group A_n is generated by its 3-cycles.

Proof. Let π be an element of A_n. By Corollary 7.13, π can be written as a product of an even number of transpositions. So, it is enough to show that any product of two different transpositions can be written as a product of 3-cycles. Let us consider the product $(i,j)(r,s)$:

If the four integers i, j, r, s are distinct, then

$$(i,j)(r,s) = (i,r,j)(i,r,s) .$$

Otherwise, we may assume without loss of generality that $i = r$, in which case

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

⊣

Let us now consider the centres of S_n and A_n. Since $S_1 = A_1 \cong A_2 \cong C_1$, $Z(S_1) = Z(A_1) \cong Z(A_2) = \{\iota\}$. Further, $S_2 \cong C_2$ and $A_3 \cong C_3$, which implies that S_2 and A_3 are abelian, and therefore, $Z(S_2) = S_2$ and $Z(A_3) = A_3$. In general, we get the following:

Theorem 7.15.
(a) For any $n \geq 3$, $Z(S_n) = \{\iota\}$.
(b) For any $n \geq 4$, $Z(A_n) = \{\iota\}$.

Proof. (a) Let $\sigma \in S_n$ be any permutation except the identity: Since $\sigma \neq \iota$, there is an $i \in \{1, \dots, n\}$ such that $\sigma(i) = j \neq i$. Pick any $k \in \{1, \dots, n\}$ distinct from i and j. Now, $\sigma\,(i,k)\,\sigma^{-1} = \big(j, \sigma(k)\big) \neq (i,k)$, since $j \notin \{i,k\}$. Hence, $\sigma\,(i,k) \neq (i,k)\,\sigma$, which implies that $\sigma \notin Z(S_n)$.

(b) Let $\pi \in A_n$ be any permutation except the identity: Since $\pi \neq \iota$, there is an $i \in \{1, \dots, n\}$ such that $\pi(i) = j \neq i$. Pick any distinct $k, \ell \in \{1, \dots, n\}$, both distinct from i and j. Now, $\pi\,(i,k,\ell)\,\pi^{-1} = \big(j, \pi(k), \pi(\ell)\big) \neq (i,k,\ell)$, since $j \notin \{i,k,\ell\}$. Hence, $\pi\,(i,k,\ell) \neq (i,k,\ell)\,\pi$, which implies that $\pi \notin Z(A_n)$. ⊣

Finally, let us consider the automorphism group of S_n:

For any group G and for any $x \in G$, the mapping $\varphi_x : G \to G$ defined by $\varphi_x(a) := xax^{-1}$ is an automorphism of G (*cf.* Hw8.Q38). Such an automorphism is called an **inner automorphism** of G. Let $\mathrm{Inn}(G)$ denote the set of all inner automorphisms of G. Further, the mapping $\psi : G \to \mathrm{Aut}(G)$ defined by $\psi(x) := \varphi_x$ is a homomorphism from G to $\mathrm{Aut}(G)$, which implies that $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$ and, by the First Isomorphism Theorem, that $G/Z(G) \cong \mathrm{Inn}(G)$ (*cf.* Hw10.Q46).

Let us turn back to the group S_n. As an immediate consequence of Theorem 7.15 we get the following:

Proposition 7.16. For any $n \geq 3$, $\mathrm{Inn}(S_n) \cong S_n$.

In the following we will show that for any $n \geq 3$, where $n \neq 6$, every automorphism of S_n is an inner automorphism. Let us first consider what an automorphism is doing with transpositions.

Lemma 7.17. Let $n \geq 3$, where $n \neq 6$, $\varphi \in \mathrm{Aut}(S_n)$ and (i,j) a transposition in S_n. Then $\varphi(i,j)$ is a transposition.

Proof. The transposition (i,j) has order 2, and therefore, $\varphi(i,j)$ has order 2 (see Hw9.Q44 (c)). Thus, $\varphi(i,j)$ must be the product of r disjoint transpositions where $2r \leq n$. There are $\binom{n}{2}$ transpositions in S_n, and there are

$$\underbrace{\binom{n}{2} \cdot \binom{n-2}{2} \cdot \;\ldots\; \cdot \binom{n-2(r-1)}{2}}_{r \text{ factors}} \cdot \frac{1}{r!}$$

products of r disjoint transpositions. Now, if $\varphi\big((i,j)\big)$ is a product of r disjoint transpositions, then for every transposition (k,ℓ), $\varphi\big((k,\ell)\big)$ is also a product of r disjoint transpositions. Indeed, by Proposition 7.6 there exists a permutation ρ such that $\rho\,(i,j)\,\rho^{-1} = (k,\ell)$, and since φ is an automorphism we get $\varphi\big(\rho\,(i,j)\,\rho^{-1}\big) = \varphi(\rho)\,\varphi\big((i,j)\big)\,\varphi(\rho)^{-1} = \varphi\big((k,\ell)\big)$, and therefore, by Proposition 7.6 again, $\varphi\big((i,j)\big)$ has the same cycle structure as $\varphi\big((k,\ell)\big)$. So, the number of transpositions in S_n must correspond to the number of products of r disjoint transpositions in S_n. In other words, we must have

$$\frac{n(n-1)}{2} = \frac{n(n-1)(n-2) \cdot \ldots \cdot (n-2r+1)}{2^r \cdot r!},$$

or equivalently,

$$2^{r-1} \cdot r! = (n-2)(n-3) \cdot \ldots \cdot (n-2r+1)\,. \tag{$*$}$$

Obviously, equation ($*$) holds for $r = 1$. So, let us consider the other cases:

For $r = 2$ we get $4 = (n-2)(n-3)$, which is impossible.

For $r = 3$ we get $24 = (n-2)(n-3)(n-4)(n-5)$ which holds just for $n = 6$, but we excluded this case.

For $n \geq 4$ we get

$$(n-2)(n-3) \cdot \ldots \cdot (n-2r+1) \underset{\substack{\uparrow \\ n \geq 2r}}{\geq} (2r-2)(2r-3) \cdot \ldots \cdot 1 = (2r-2)! =$$

$$= \underbrace{(2r-2) \cdot \ldots \cdot (r+1)}_{r-2 \text{ factors, each } > 4} \cdot r! \geq 4^{r-2} \cdot r! = 2^{2(r-2)} \cdot r! > 2^{r-1} \cdot r!\,,$$

which shows that also in this case the equation ($*$) does not hold.

Thus, $r = 1$, or in other words, $\varphi\big((i,j)\big)$ is a transposition. $\dashv$

THEOREM 7.18. Let $n \geq 3$, where $n \neq 6$, then $\mathrm{Aut}(S_n) \cong S_n$.

Proof. By Proposition 7.16 it is enough to show that every automorphism of S_n is an inner automorphism. By Proposition 7.8 we know that S_n is generated by the transpositions $(1,2)$, $(1,3), \ldots, (1,n)$, so, it is enough to consider these transpositions. By Lemma 7.17 we know that for any $\varphi \in \mathrm{Aut}(S_n)$ and for any $i \in \{2,\ldots,n\}$, $\varphi\big((1,i)\big)$ is a transposition. Pick any two distinct numbers i, j from the set $\{2,3,\ldots,n\}$ and let

$$\varphi\big((1,i)\big) = (k,\ell) \text{ and } \varphi\big((1,j)\big) = (p,q)\,.$$

Now, $(1,i)(1,j) = (1,j,i)$ and has order 3, and hence, $(k,\ell)(p,q)$ must also have order 3, which implies that two of the four element k,ℓ,p,q must be equal. Without loss of generality, let us assume that $p = k$. Then $\varphi\big((1,i)\big) = (k,\ell)$ and $\varphi\big((1,j)\big) = (k,q)$. If $n > 3$, then we can pick an number $h \in \{1,\ldots,n\} \setminus \{1,i,j\}$. Let $\varphi\big((1,h)\big) = (r,s)$, then $\{r,s\}$ has one element in common with $\{k,\ell\}$ and with $\{k,q\}$. If $r = \ell$ and $s = q$, then we would have

$$\begin{aligned}\varphi\big((1,j,i)\big) = \varphi\big((1,i)(1,j)\big) = (k,\ell)(k,q) = (k,q,\ell) = \\ = (q,\ell,k) = (k,q)(\ell,q) = \varphi\big((1,j)(1,h)\big) = \varphi\big((1,h,j)\big)\,,\end{aligned}$$

but this is a contradiction since φ is injective and $(1,j,i) \neq (1,h,j)$. So, we have either $r = k$ or $s = k$.

In general, for every $i \in \{2,\ldots,n\}$ there exists a unique $\pi(i) \in \{1,\ldots,n\} \setminus \{k\}$ such that

$$\varphi\big((1,i)\big) = \big(k,\pi(i)\big)\,.$$

Further, it is not hard to see that we stipulate $\pi(1) := k$, then π is a permutation of $\{1,\ldots,n\}$. Hence, by Proposition 7.6 we finally have

$$\varphi\big((1,i)\big) = \big(k,\pi(i)\big) = \big(\pi(1),\pi(i)\big) = \pi\,(1,i)\,\pi^{-1}\,,$$

which shows that every automorphism of S_n is an inner automorphism, which completes the proof. $\dashv$

What about $\mathrm{Aut}(S_6)$? One can show that there exists an automorphism $\varphi \in \mathrm{Aut}(S_6)$ such that $\varphi(i,j)$ is the product of 3 disjoint transpositions, and hence, by Proposition 7.6, $\varphi \notin \mathrm{Inn}(S_6)$. Moreover one can show that $|\,\mathrm{Aut}(S_6)| = 1440$, and since $\mathrm{Inn}(S_6) \cong S_6$ and $|S_6| = 720$, this implies that $|\,\mathrm{Aut}(S_6) : \mathrm{Inn}(S_6)| = 2$, and therefore $\mathrm{Inn}(S_6) \lhd \mathrm{Aut}(S_6)$ (we omit the proof).