19. Automorphism group of S_n

Definition-Lemma 19.1. *Let G be a group.*

*The **automorphism group of** G, denoted $\operatorname{Aut}(G)$, is the subgroup of $A(G)$ of all automorphisms of G.*

Proof. We check that $\operatorname{Aut}(G)$ is closed under products and inverses.

Suppose that ϕ and $\psi \in \operatorname{Aut}(G)$. Let $\xi = \phi \circ \psi$. If g and $h \in G$ then

$$\begin{aligned}\xi(gh) &= (\phi \circ \psi)(gh)\\ &= \phi(\psi(gh))\\ &= \phi(\psi(g)\psi(h))\\ &= \phi(\psi(g))\phi(\psi(h))\\ &= (\phi \circ \psi)(g)(\phi \circ \psi)(h)\\ &= \xi(g)\xi(h).\end{aligned}$$

Thus $\xi = \phi \circ \psi$ is a group homomorphism. Thus $\operatorname{Aut}(G)$ is closed under products.

Now let $\xi = \phi^{-1}$. If g and $h \in G$ then we can find g' and h' such that $g = \phi(g')$ and $h = \phi(h')$. It follows that

$$\begin{aligned}\xi(gh) &= \xi(\phi(g')\phi(h'))\\ &= \xi(\phi(g'h'))\\ &= g'h'\\ &= \xi(g)\xi(h).\end{aligned}$$

Thus $\xi = \phi^{-1}$ is a group homomorphism. Thus $\operatorname{Aut}(G)$ is closed under inverses. □

Lemma 19.2. *Let G be a group and let $a \in G$. ϕ_a is the automorphism of G given by conjugation by a, $\phi(g) = aga^{-1}$.*

If a and $b \in G$ then

$$\phi_{ab} = \phi_a\phi_b.$$

Proof. Both sides are functions from G to G. We just need to check that they have the same effect on any element g of G:

$$\begin{aligned}(\phi_a \circ \phi_b)(g) &= \phi_a(\phi_b(g))\\ &= \phi_a(bgb^{-1})\\ &= a(bgb^{-1})a^{-1}\\ &= (ab)g(ab)^{-1}\\ &= \phi_{ab}(g).\end{aligned}$$ □

Definition-Lemma 19.3. *We say that an automorphism ϕ of G is* ***inner*** *if $\phi = \phi_a$ for some a. The* ***inner automorphism group*** *of G, denoted* $\operatorname{Inn}(G)$, *is the subgroup of* $\operatorname{Aut}(G)$ *given by inner automorphisms.*

Proof. We check that $\operatorname{Inn}(G)$ is closed under products and inverses.

We checked that $\operatorname{Inn}(G)$ is closed under products in (19.2). Suppose that $a \in G$. We check that the inverse of ϕ_a is $\phi_{a^{-1}}$. We have

$$\begin{aligned} \phi_a \phi_{a^{-1}} &= \phi_{aa^{-1}} \\ &= \phi_e, \end{aligned}$$

which is clearly the identity function. Thus $\operatorname{Inn}(G)$ is closed under inverses. □

Definition-Lemma 19.4. *Let G be a group.*

Then the inner automorphism group is a normal subgroup of $\operatorname{Aut}(G)$. *The quotient group* $\operatorname{Aut}(G)/\operatorname{Inn}(G)$ *is called the* ***outer automorphism group of*** *G, denoted* $\operatorname{Out}(G)$.

Proof. Let f be an automorphism of G and let ϕ_a be an inner automorphism. Let $b = f(a)$. We check $f\phi_a f^{-1} = \phi_b$. Since both sides are functions from G to G we just need to check they have the same effect on every element g of G. Suppose that $g = f(h)$. We have

$$\begin{aligned} (f\phi_a f^{-1})(g) &= (f\phi_a f^{-1})(f(h)) \\ &= f\phi_a(h) \\ &= f(aha^{-1}) \\ &= f(a)f(h)f(a^{-1}) \\ &= bgb^{-1} \\ &= \phi_b(g). \end{aligned}$$

□

Lemma 19.5. *Let G be a group with centre Z.*

Then $\operatorname{Inn}(G) \simeq G/Z$.

Proof. Define a function

$$A \colon G \longrightarrow \operatorname{Inn}(G) \qquad \text{by sending} \qquad a \longrightarrow \phi_a.$$

A is a group homomorphism by (19.2). A is clearly surjective. We identify the kernel. $a \in \operatorname{Ker} A$ if and only if ϕ_a is the identity if and only if $\phi_a(g) = g$ for all $g \in G$ if and only if $aga^{-1} = g$ for all $g \in G$ if and only if $ag = ga$ for all $g \in G$ if and only if $a \in Z$.

Now apply the first Isomorphism Theorem. □

Theorem 19.6. $\operatorname{Aut}(S_n) = \operatorname{Inn}(S_n) \simeq S_n$ *unless*

(1) $n = 2$ *when* $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n) = \{e\}$.
(2) $n = 6$ *when* $\mathrm{Inn}(S_n) = S_n$ *and* $\mathrm{Out}(S_n) = \mathbb{Z}_2$.

Observe that (19.6) says that most automorphisms of S_n are inner. We first compute the centre of S_n:

Lemma 19.7. *The centre of* S_n *is* $\{e\}$ *unless* $n = 2$.

Proof. We may assume that $n \geq 3$. Suppose that $\sigma \in S_n$ is not the identity. Pick i such that $j = \sigma(i) \neq i$. Pick $k \notin \{i, j\}$ and let $\tau = (j, k)$. Then $\tau\sigma\tau^{-1}$ sends i to k. Thus

$$\tau\sigma\tau^{-1} \neq \sigma,$$

so that σ does not belong to the centre. □

Note that an inner automorphism of S_n preserves cycle type. We show the converse is true.

Lemma 19.8. *If* ϕ *is an automorphism of a group* G *then* ϕ *permutes the conjugacy classes of* G.

Proof. Let $\sim$ be the relation $a \sim b$ if and only if a and b are conjugate.

Suppose that $a \sim b$. Then we may find $g \in G$ such that $b = gag^{-1}$. We have

$$\begin{aligned}\phi(b) &= \phi(gag^{-1}) \\ &= \phi(g)\phi(a)\phi(g^{-1}) \\ &= \phi(g)\phi(a)\phi(g)^{-1},\end{aligned}$$

so that $\phi(a) \sim \phi(b)$. It follows that ϕ sends equivalence classes to equivalence classes. But these are just the conjugacy classes. □

Lemma 19.9. *Suppose that* G *is a group and* S *is a set of generators of* G.

If ϕ_1 *and* ϕ_2 *are two automorphisms of* G *that agree on* S *then* $\phi_1 = \phi_2$.

Proof. Let H be the largest subset of G on which ϕ_1 and ϕ_2 agree. We show that H is a subgroup of G. $e \in H$ and so H is non-empty. Suppose that g and h belong to H. We have

$$\begin{aligned}\phi_1(gh) &= \phi_1(g)\phi_1(h) \\ &= \phi_2(g)\phi_2(h) \\ &= \phi_2(gh).\end{aligned}$$

Thus $gh \in H$. Thus H is closed under products.

Suppose that $g \in H$. We have

$$\begin{aligned}\phi_1(g^{-1}) &= \phi_1(g)^{-1} \\ &= \phi_2(g)^{-1} \\ &= \phi_2(g^{-1}).\end{aligned}$$

Thus $g^{-1} \in H$ and so H is closed under inverses. Thus H is a subgroup of G.

As H contains S, $H = G$, and so $\phi_1 = \phi_2$. □

Lemma 19.10. *Let $\sigma = (a, b)$ and $\tau = (c, d)$ be two transpositions in S_n.*

Then σ and τ commute if and only if $I = \{a, b, c, d\}$ does not have three elements.

Proof. If I has two elements then $\sigma = \tau$ and they obviously commute. If I has four elements then σ and τ are disjoint transpositions and they obviously commute.

If I has three elements then $\sigma\tau$ and $\tau\sigma$ are two three cycles. But one is the inverse of the other so they are not equal. □

Lemma 19.11. *If $\phi \in \mathrm{Aut}(S_n)$ sends transpositions to transpositions then ϕ is inner.*

Proof. The transpositions $(i, i+1)$, $1 \leq i \leq n-1$ generate S_n.

Suppose that $(\alpha, \beta) = \phi(i, i+1)$ and $(\gamma, \delta) = \phi(i+1, i+2)$. As $\{i, i+1, i+2\}$ has cardinality three it follows that $(i, i+1)$, $(i+1, i+2)$ do not commute. But then (α, β) and (γ, δ) don't commute. It follows that $\{\alpha, \beta, \gamma, \delta\}$ has three elements. Possibly rearranging we may assume that $\beta = \gamma$. Thus we may assume that there are $a_1, a_2, \dots, a_n$ such that $(a_i, a_{i+1}) = \phi(i, i+1)$. Let $\tau(i) = a_i$. Then τ is a permutation of the first n natural numbers and ϕ and ϕ_τ agree on the generators $(i, i+1)$. (19.9) implies that $\phi = \phi_\tau$ so that ϕ is inner. □

Lemma 19.12. *Let $C \subset S_n$ be a conjugacy class with $\binom{n}{2}$ elements of order 2.*

Then either C consists of transpositions or $n = 6$ and C consists of the product of three disjoint transpositions.

Proof. The only perumutations of order two are the product of k disjoint transpositions. In this case the cycle type is $1^{n-2k}2^k$. Conjugacy in S_n is determined by cycle type. The number of permutations with cycle type 2^k is

$$\frac{1}{k!}\binom{n}{2}\binom{n-2}{2}\cdots\binom{n+2-2k}{2}.$$

For this to equal $\binom{n}{2}$ we must have

$$\frac{1}{(k-1)!}\binom{n-2}{2}\dots\binom{n+2-2k}{2}=k.$$

Note that the LHS counts the number of permutations with cycle type $1^{n-2k}2^{k-1}$.

If $k=1$ then both sides are equal to one. So suppose $k\geq 2$. As $k>1$, the number of permutations in S_{n-2} which are the product of $k-1$ disjoint transpositions is at least the number of ways to pair the first element with any other element, which is $n-2-1=n-3$. So we must have $n-3\leq k$, that is, $n\leq k+3$.

As $2k\leq n$ we must have $k\leq 3$. In this case $n\leq 6$. If $k=3$ then $n=6$ and we get equality. If $k=2$ then $4\leq n\leq 5$. If $n=4$ the LHS is 1, not 2, and if $n=5$ the LHS is 3, not 2. □

If we put everything we have done together it remains to show that if $n=6$ then the outer automorphism is non-trivial.

Lemma 19.13. *The order of* $\operatorname{Out}(S_6)$ *is at most two.*

Further the order is two if and only if there is an automorphism ϕ of S_6 which sends a transposition to a product of three disjoint transpositions.

Proof. We have already seen that an automorphism is inner if it fixes the subset of all transpositions. By (19.12) if we don't send a transposition to a transposition then we must send it to product of three disjoint transpositions. □

It is actually suprisingly involved to write down an automorphism ϕ which sends a transposition to a product of three disjoint transpositions. The problem is that there are too many choices. Outer automorphisms are really equivalence classes, left cosets of the inner automorphism group. Writing down an explicit automorphism which is not inner is somehow completely the opposite to what we have have done so far, there don't seem to be any natural choices.

In our case there are $6!=720$ inner automorphisms and so ϕ belongs to a left coset with 720 elements. We start by figuring out how ϕ acts on the other conjugacy classes. It is useful to write down a table of conjugacy classes, the order of a typical element and their sizes:

Type	Order	Size
e	1	1
$(1,2)$	2	15
$(1,2)(3,4)$	2	45
$(1,2)(3,4)(5,6)$	2	15
$(1,2,3)$	3	40
$(1,2,3)(4,5,6)$	3	40
$(1,2,3,4)$	4	90
$(1,2,3,4)(5,6)$	4	90
$(1,2,3,4,5)$	5	144
$(1,2,3,4,5,6)$	6	120
$(1,2)(3,4,5)$	6	120

As a check, the sum of the numbers in the last column is $720 = 6!$ the order of S_n.

Note that all of these conjugacy classes come in pairs C_1 and C_2, where the order of the elements of C_1 and C_2 are the same and the cardinality of C_1 and C_2 is the same, with three exceptions. Presumably an outer automorphism switches C_1 and C_2. $(1,2)$ is paired with $(1,2)(3,4)(5,6)$; $(1,2,3)$ is paired with $(1,2,3)(4,5,6)$; $(1,2,3,4)$ is paired with $(1,2,3,4)(5,6)$; $(1,2,3,4,5,6)$ is paired with $(1,2,3)(4,5)$. The classes represented by e, $(1,2)(3,4)$ and $(1,2,3,4,5)$ are paired with themselves. This suggests that 5-cycles play a special role.

The construction of an outer automorphism is quite involved; the interested reader might look online for all of the details. The idea is to find an injective group homomorphism $\pi\colon S_5 \longrightarrow S_6$ which is different from the obvious inclusion.

Take the complete graph with 5 vertices and colour the ten edges red and blue so that there is one red 5-cycle and one blue 5-cycle. After a little bit of drawing pictures, it is not hard to see there are six ways to do this (we consider a red-blue colouring and blue-red colouring the same). Permuting the five vertices permutes the six ways to colour. This defines π.

Note that the kernel of π is one of the following normal subgroups: $\{e\}$, A_5 and S_5. It is not hard to check that $(1,2,3) \in A_5$ is not in the kernel so that the kernel is $\{e\}$ and so π is injective. It is also not hard to see that the transposition $(1,2)$ is sent to a product of three disjoint transpositions.

Let H be the image of S_5. Then H is a subgroup of S_6 of index $6 = 6!/5!$. S_6 acts on the left cosets of H in S_6 and this defines a homomorphism $\phi\colon S_6 \longrightarrow S_6$. Again the kernel is one of three possible normal subgroups $\{e\}$, A_6 or S_6. It is again easy to see the kernel of ϕ is $\{e\}$. It follows that ϕ is injective, so that ϕ is a bijection. Once again, it is not hard to check that the image of a transposition is not a transposition, it is product of three disjoint transpositions, so that ϕ corresponds to an outer automorphism.

Note one peculiar facet of the proof. We construct an isomorphism $S_6 \longrightarrow S_6$, but the two copies of S_6 are not the same. The first S_6 is the group of permutations of the red-blue colourings of the complete graph with five vertices. The second S_5 are the left cosets of H inside S_6.

To get an actual automorphism of S_6 we need to pick an identification of the two copies of S_6. If we pick a way to identify the first six objects with the second six objects then we get an identification of the two copies of S_6. This gives an automorphism of S_6, which is indeed outer.

The ambiguity in the choice of identification is exactly given by the inner automorphisms of one copy of S_6. Let G_1 and G_2 be the two copies of S_6. Suppose we are given two isomorphisms,

$$f\colon G_1 \longrightarrow G_2 \qquad \text{and} \qquad g\colon G_1 \longrightarrow G_2.$$

Then the composition $\alpha = g^{-1} \circ f$ is an automorphism of G_1. Conversely given an automorphism α of G_1, and an identification $g\colon G_1 \longrightarrow G_2$ then $f = \alpha \circ g\colon G_1 \longrightarrow G_2$ is another identification.