

# Group Theory - Weeks 8 - Alternating Groups

Antonio León Villares

November 2022

## Contents

|          |                                                                    |          |
|----------|--------------------------------------------------------------------|----------|
| <b>1</b> | <b>Symmetric Groups</b>                                            | <b>2</b> |
| 1.1      | Definition: Symmetric Group . . . . .                              | 2        |
| 1.2      | Lemma: Permutations as Products of Disjoint Cycles . . . . .       | 2        |
| 1.3      | Transpositions . . . . .                                           | 2        |
| 1.3.1    | Definition: Transposition . . . . .                                | 2        |
| 1.3.2    | Lemma: Permutations as Products of Transpositions . . . . .        | 3        |
| 1.3.3    | Definition: Even and Odd Permutations . . . . .                    | 3        |
| 1.3.4    | Lemma: Parity of Product of Permutations . . . . .                 | 3        |
| 1.4      | Conjugate Permutations . . . . .                                   | 4        |
| 1.4.1    | Definition: Cycle Type . . . . .                                   | 4        |
| 1.4.2    | Lemma: Effect of Conjugating Permutations . . . . .                | 4        |
| 1.4.3    | Theorem: Conjugate Permutations Have the Same Cycle Type . . . . . | 4        |
| <b>2</b> | <b>Alternating Groups</b>                                          | <b>4</b> |
| 2.1      | Definition: The Alternating Group (1) . . . . .                    | 4        |
| 2.2      | Definition: The Alternating Group (2) . . . . .                    | 5        |
| 2.3      | Theorem: The Alternating Group is a Normal Subgroup . . . . .      | 5        |
| 2.4      | The Alternating Groups $A_4$ and $A_5$ . . . . .                   | 6        |
| 2.4.1    | Recap: Conjugacy Classes and Centralizers . . . . .                | 6        |
| 2.4.2    | Lemma: Normal Groups are Unions of Conjugacy Classes . . . . .     | 7        |
| 2.4.3    | Proposition: Properties of $A_4$ . . . . .                         | 7        |
| 2.4.4    | Theorem: $A_5$ is Simple . . . . .                                 | 9        |
| 2.5      | Simplicity of the Alternating Groups . . . . .                     | 12       |
| 2.5.1    | Lemma: 3-Cycles are Conjugate in Alternating Groups . . . . .      | 12       |
| 2.5.2    | Lemma: 3-Cycles Generate Alternating Groups . . . . .              | 13       |
| 2.5.3    | Lemma: Order of Fixed-Point-Free Subgroups . . . . .               | 13       |
| 2.5.4    | Lemma: Order of Conjugacy Classes of Alternating Groups . . . . .  | 13       |
| 2.5.5    | Theorem: Alternating Groups are Simple When $n \geq 5$ . . . . .   | 14       |

# 1 Symmetric Groups

## 1.1 Definition: Symmetric Group

The **symmetric group**  $S_n$  is the **group** containing all **bijections** (also known as **permutations**):

$$\sigma : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$$

We often represent **permutations** via **cycle notation**:

$$(1243) \iff \left\{ \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 4 \\ 4 \mapsto 3 \\ 3 \mapsto 1 \end{array} \right\}$$

## 1.2 Lemma: Permutations as Products of Disjoint Cycles

Every **permutation** can be written as a **product of disjoint cycles**. This product is **unique** up to re-ordering of the factors. (Lemma 6.1.1)

## 1.3 Transpositions

### 1.3.1 Definition: Transposition

A **transposition** is a **2-cycle**. That is, a cycle containing only 2 elements.

An **adjacent transposition** is a **transposition** of the form  $(i \ i + 1)$ .

### 1.3.2 Lemma: Permutations as Products of Transpositions

$S_n$  is **generated** by **transpositions**.

That is, **every** permutation can be written as a **product of transpositions**.

---

For instance:

$$(1243) = (13)(14)(12)$$

(Lemma 6.1.2)

### 1.3.3 Definition: Even and Odd Permutations

A **permutation** is **even** if it can be written as a **product of an even number of transpositions**.

If it is **odd** otherwise.

The **identity** permutation is **even** (it is written as a product of 0 transpositions)

---

For instance:

$$(1243) = (13)(14)(12)$$

is **even**, whilst:

$$(154)(23) = (14)(15)(23)$$

is **odd**.

---

In particular, this means that if  $\sigma$  has **odd** cycle length, it is an **even** permutation, whilst if the cycle length is **even**,  $\sigma$  is **odd**.

### 1.3.4 Lemma: Parity of Product of Permutations

The product of:

- 2 **even** permutations
- 2 **odd** permutations

is **even**.

The product of an **odd** and an **even** permutation is **odd**.

## 1.4 Conjugate Permutations

### 1.4.1 Definition: Cycle Type

Let:

$$\sigma = c_1 c_2 \dots c_k$$

be a **product** of  $k$  **disjoint** cycles of length:

$$l_1, l_2, \dots, l_k, \quad l_1 \geq l_2 \geq \dots \geq l_k$$

Then, the **cycle type** of  $\sigma$  is the  $k$ -tuple:

$$(l_1, l_2, \dots, l_k)$$

(Definition 6.1.3)

### 1.4.2 Lemma: Effect of Conjugating Permutations

Let:

$$\sigma = (a_1 \ a_2 \ \dots \ a_k) \in S_n$$

and  $\tau \in S_n$ .

Then:

$$\tau \sigma \tau^{-1} = (\tau(a_1) \ \tau(a_2) \ \dots \ \tau(a_k))$$

(Lemma 6.1.7)

### 1.4.3 Theorem: Conjugate Permutations Have the Same Cycle Type

Two **permutations** in  $S_n$  are **conjugate if and only if** they have the **same cycle type**.

(Theorem 6.1.8)

## 2 Alternating Groups

### 2.1 Definition: The Alternating Group (1)

The **alternating group** is a the **subgroup**  $A_n \leq S_n$  containing all the **even** permutations of  $S_n$ .

## 2.2 Definition: The Alternating Group (2)

Let  $x_1, \dots, x_n$  be variables, and define an object:

$$P = \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

If  $X = \{P, -P\}$ ,  $S_n$  acts on  $X$  via:

$$\sigma \cdot P = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)})$$

In particular, if  $\sigma$  is **even**:

$$\sigma \cdot P = P$$

and if  $\sigma$  is **odd**:

$$\sigma \cdot P = -P$$

---

Hence,  $A_n$  is the **stabiliser** of the **action** of  $S_n$  on  $X$ .

## 2.3 Theorem: The Alternating Group is a Normal Subgroup

Let  $n \geq 2$ . Then  $A_n \triangleleft S_n$ , and:

$$|S_n| = 2|A_n| \implies |A_n| = \frac{n!}{2}$$

(Theorem 6.2.3)

---

*Proof.* By definition,  $A_n$  is the stabiliser of the action of  $S_n$  on  $X$ , so by the Orbit-Stabilizer Theorem:

$$|S_n| = |\text{Stab}_{S_n}(P)| |\text{Orb}_{S_n}(P)|$$

The orbit of  $P$  over  $S_n$  is clearly  $X$  (since  $n \geq 2$ ,  $S_n$  contains the identity (**even** permutation) and a transposition (**odd** permutation)).

Hence:

$$|S_n| = 2|A_n|$$

as required.

We now show that  $A_n$  is a normal subgroup. Define a homomorphism:

$$\text{sgn} : S_n \rightarrow C_2$$

$$\text{sgn}(\sigma) = \begin{cases} 1, & \sigma \text{ is even} \\ -1, & \sigma \text{ is odd} \end{cases}$$

If  $\sigma, \tau$  have the same parity, their product is even, so:

$$\text{sgn}(\sigma\tau) = 1 = \text{sgn}(\sigma)\text{sgn}(\tau)$$

Otherwise, their product is odd:

$$\text{sgn}(\sigma\tau) = -1 = \text{sgn}(\sigma)\text{sgn}(\tau)$$

so  $\text{sgn}$  is indeed a homomorphism.

Moreover, by definition of  $A_n$ :

$$\ker(\text{sgn}) = A_n$$

Since the kernel of a homomorphism is a **normal subgroup**, it follows that  $A_n$  is a normal subgroup of  $S_n$ .  $\square$

## 2.4 The Alternating Groups $A_4$ and $A_5$

We choose to focus on  $A_4$  and  $A_5$  because if  $n \leq 3$ , the alternating groups are rather uninteresting:

$$S_1 = \{\iota\} \implies A_1 = \{\iota\}$$

$$S_2 = \{\iota, (12)\} \implies A_2 = \{\iota\}$$

$$S_3 = \{\iota, (12), (23), (13), (123) = (13)(12), (132) = (12)(13)\} \implies A_3 = \{\iota, (123), (132)\}$$

It is once we look at  $A_4$  and  $A_5$  that we see interesting behaviour. In fact, it is this behaviour which leads to proving that polynomials of degree  $\leq 4$  can be solved by radicals, whilst polynomials with degree  $\geq 5$  can't!

### 2.4.1 Recap: Conjugacy Classes and Centralizers

If we let  $G$  act on itself via conjugation:

$$g \cdot a = gag^{-1}$$

we can define the **conjugacy classes** of a **group**, alongside the **centralisers**.

Let  $G$  be a group. The **conjugacy class** of  $a \in G$  is the **orbit** of  $a$ :

$$Cl(a) = Orb_G(a) = \{gag^{-1} \mid g \in G\}$$

Let  $G$  be a group. The **centralizer** of  $a \in G$  is the **stabilizer** of  $a$ :

$$C_G(a) = Stab_G(a) = \{g \mid gag^{-1} = a, g \in G\} = \{g \mid ga = ag, g \in G\}$$

That is, the **centralizer** of  $a$  is the set of all elements in  $G$  which **commute** with  $a$ .

Let  $G$  be a finite group. By the Orbit-Stabilizer Theorem:

$$\forall a \in G, \quad |G| = |C_G(a)| |Cl(a)|$$

(Lemma 4.2.7)

### 2.4.2 Lemma: Normal Groups are Unions of Conjugacy Classes

Let  $G$  be a **finite group**, and suppose that:

$$H \triangleleft G$$

Then,  $\exists h_1, \dots, h_k \in H$  such that:

$$H = \sqcup_{i=1}^k Cl_G(h_i)$$

That is, a **normal subgroup** can be described as the **disjoint union** of **conjugacy classes**.  
(Lemma 6.2.5)

*Proof.* Let  $H \triangleleft G$ . Then:

$$\forall g \in G, \quad gHg^{-1} = H$$

Now, let  $h_i \in H$ . The **conjugacy class** of  $h_i$  is the set of all elements in  $G$  which are conjugate to  $h_i$ :

$$Cl(h_i) = \{gh_i g^{-1} \mid g \in G\} \subseteq H$$

But now, conjugacy classes are disjoint (they are equivalence classes under the equivalence relation of conjugation), so there must exist representatives in  $H$ , such that the disjoint union of their conjugacy classes create  $H$ . □

### 2.4.3 Proposition: Properties of $A_4$

The following are properties of  $A_4$ :

1.

$$|A_4| = 12$$

2.  $A_4$  has a **unique** subgroup  $N$  of order 4

3.

$$N \triangleleft S_4 \quad \text{and} \quad N \triangleleft A_4$$

4.

$$A_4/N \cong C_3 \quad \text{and} \quad S_4/N \cong S_3$$

*Proof.* 1.  $|A_4| = 12$

This follows immediately:

$$|A_4| = \frac{4!}{2} = 12$$

2. The cycle types of elements in  $S_4$  are:

- 4 (odd)
- 3,1 (even)
- 2,2 (even)
- 2,1,1 (odd)
- 1,1,1,1 (even)

Moreover, by Sylow I,  $|A_4| = 12 = 4 \times 3$  has a Sylow 2-subgroup of order 4, call it  $N$ . Furthermore, by Lagrange's Theorem, elements in  $N$  must have an order which divides 4, so  $\sigma \in N \implies o(\sigma) \in \{1, 2, 4\}$ . Finally, the order of a permutation is the lcm of cycle lengths of its disjoint cycle decomposition. Hence, this tells us that elements in  $N$  must have cycle type (2, 2) or 4 (the identity is obviously in  $N$ ). However, notice that the elements with cycle length 4 are odd permutations, so they aren't even part of  $A_4$ . Hence, there is a **unique** subgroup of order 4, and it must be formed by the elements of  $S_4$  with cycle shape (2, 2). That is:

$$N = \{e, (12)(34), (13)(24), (14)(23)\}$$

which indeed has 4 elements, as expected.

3.  $N \triangleleft S_4, N \triangleleft A_4$

Clearly,  $N$  must be normal, since it is the unique Sylow 2-subgroup of  $A_4$ . It is also a subgroup of  $S_4$ . It will be a normal subgroup of  $S_4$  because  $N$  contains all elements of cycle type (2, 2), so in particular, they are all conjugate. Since a normal subgroup is a disjoint union of conjugacy classes,  $N$  must still be a normal subgroup of  $S_4$ .

4.  $A_4/N \cong C_3, S_4/N \cong S_3$

By Lagrange's Theorem:

$$|A_4/N| = \frac{12}{4} = 3$$

Hence,  $A_4/N$  is a group of order 3. 3 is prime, so by Lagrange's Theorem,  $A_4/N$  is a cyclic group of order 3, so  $A_4/N \cong C_3$ .

Similarly,

$$|S_4/N| = \frac{24}{4} = 6$$

so  $S_4/N$  is a group of order 6. There are only 2 groups of order 6:  $C_6$  and  $S_3$ . However, since  $S_4$  isn't abelian,  $S_4/N$  won't be abelian. For instance, if we pick  $\alpha = (12)$  and  $\beta = (14)$ , then:

$$\alpha N * \beta N = (\alpha \circ \beta)N = (142)N$$

$$\beta N * \alpha N = (\beta \circ \alpha)N = (124)N$$

Hence, the  $S_4/N \cong S_3$ .

□



#### 2.4.4 Theorem: $A_5$ is Simple

*The **alternating group**  $A_5$  is a **simple group**.  
(Theorem 6.3.1)*

*Proof.* We will make use of the following table of cycle types in  $S_5$ :

| Cycle Type | Number of Permutations | Even/Odd |
|------------|------------------------|----------|
| 5          | 24                     | E        |
| 4,1        | -                      | O        |
| 3,2        | -                      | O        |
| 3,1,1      | 20                     | E        |
| 2,2,1      | 15                     | E        |
| 2,1,1,1,1  | -                      | O        |
| 1,1,1,1,1  | 1                      | E        |

Counting the number of permutations of a certain cycle type is a combinatorial problem. For example, for the cycle type  $(3, 1, 1)$ , the 3 cycle has a total of  $5 \times 4 \times 3$  possibilities. However, we are overcounting:

$$(123) = (312) = (231)$$

so the possibilities for the 3 cycle are:

$$\frac{5 \times 4 \times 3}{3} = 20$$

Moreover, once we have chosen the 3-cycle, the whole permutation is decided (since the other 2 elements are fixed). For the cycle type  $(2, 2, 1)$ , the first 2-cycle has  $\frac{5 \times 4}{2} = 10$  possibilities. The second 2 cycle has  $\frac{3 \times 2}{2} = 3$  possibilities. Hence, there are  $10 \times 3 = 30$  total cycles with type  $(2, 2, 1)$ . However, notice once again we are overcounting: since the 2 cycles are disjoint, it doesn't matter which comes first, so we have  $\frac{30}{2} = 15$  cycles of type  $(2, 2, 1)$ .

To show that  $A_5$  is a simple group, we need to show that any normal subgroup will either be the trivial subgroup, or  $A_5$ . To do this, it is sufficient to compute the conjugacy classes in  $A_5$ , since their union will determine any potential normal subgroup. We need to be careful though: a conjugacy class in  $S_5$  is simply determined by the cycle type; however, in  $A_5$ , there might be permutations which won't appear.

##### ① Cycle Type 5

We first consider the conjugacy classes for permutations of cycle type 5. To do this, we exploit the Orbit-Stabilizer Theorem:

$$\forall a \in G, \quad |G| = |C_G(a)| |Cl(a)|$$

In particular, let  $\sigma = (1\ 2\ 3\ 4\ 5)$ . Using the above Theorem, alongside the fact that there are 24 elements of cycle type 5 in  $S_5$ :

$$C_{S_5}(\sigma) = |S_5|/|Cl(\sigma)| = 120/24 = 5$$

Hence, the number of elements in  $S_5$  which commute with  $\sigma$  is 5. Moreover, consider the cyclic subgroup generated by  $\sigma$ :

$$\langle \sigma \rangle = \{\sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5 = \iota\}$$

Notice, these will be the only permutations which commute with  $\sigma$  (any other permutation  $\tau \in S_5$  won't be disjoint with  $\sigma$ , and thus, won't commute). Hence:

$$\langle \sigma \rangle = C_{S_5}(\sigma)$$

Since the powers of  $\sigma$  are even permutations, they are contained in  $A_5$ , and so:

$$\langle \sigma \rangle = C_{S_5}(\sigma) = C_{A_5}(\sigma)$$

By the Orbit-Stabilizer Theorem:

$$|Cl(\sigma)| = |A_5|/|C_{A_5}(\sigma)| = 60/5 = 12$$

Now, pick  $\sigma' \in S_5$ , such that  $\sigma' \notin \langle \sigma \rangle$ . Then, by similar logic  $Cl(\sigma') = 12$ . Hence, the 2 conjugacy classes,  $Cl(\sigma), Cl(\sigma')$  will partition the conjugacy class containing elements of order 5 in  $A_5$  (since there are 24 such elements).

## ② Cycle Type (3, 1, 1)

With this cycle type, finding the centraliser is a bit harder. We can still use the Orbit-Stabilizer Theorem. Let  $\sigma$  have cycle type (3, 1, 1). Then:

$$|C_{S_5}(\sigma)| = |S_5|/|Cl(\sigma)| = 120/20 = 6$$

So we expect 6 elements of  $S_5$  to commute with  $\sigma$ . To be more concrete, let's pick a specific permutation,  $\sigma = (1\ 2\ 3)$ . Trivially, we know that  $\tau = (4\ 5)$  commutes (since they are disjoint), and  $\sigma$  also commutes. Similarly:

$$\sigma^2 = (1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2)$$

and  $\sigma^3$  will just be the identity. Since the centraliser is a subgroup, we must (at least) have that:

$$C_{S_5}(\sigma) = \{\iota, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$$

This already contains 6 commuting elements, so it must be the centraliser in  $S_5$ . But notice, some of these elements are not in  $A_5$ :  $\tau$  is odd, and so, any product containing  $\tau$  will be odd (since  $\sigma$  is even). Thus, in  $A_5$  the centraliser becomes:

$$C_{A_5}(\sigma) = \{\iota, \sigma, \sigma^2\}$$

so by the Orbit-Stabilizer Theorem:

$$|Cl(\sigma)| = |A_5|/|C_{A_5}(\sigma)| = 60/3 = 20$$

Hence, the conjugacy class for cycle type 3 permutations in  $A_5$  is the same as in  $S_5$ .

## ③ Cycle Type (2, 2, 1)

We reach the last non-trivial conjugacy class. In  $S_5$ , there are 15 elements with this cycle-type, so if  $\sigma$  has cycle type  $(2, 2, 1)$ :

$$|C_{S_5}(\sigma)| = |S_5|/|Cl(\sigma)| = 120/15 = 8$$

so we expect 8 elements to commute with  $\sigma$ . Lets consider  $\sigma = (1\ 2)(3\ 4)$ .  $\sigma$  has order 2 (since it is composed of 2 cycles of this order). Finding the remaining elements isn't as easy as above. A systematic way of checking is to use the fact that:

$$\sigma\tau = \tau\sigma \implies \tau\sigma\tau^{-1} = \sigma$$

Alongside:

*Let:*

$$\sigma = (a_1\ a_2\ \dots\ a_k) \in S_n$$

*and  $\tau \in S_n$ .*

*Then:*

$$\tau\sigma\tau^{-1} = (\tau(a_1)\ \tau(a_2)\ \dots\ \tau(a_k))$$

*(Lemma 6.1.7)*

This tells us that  $\tau$  commutes with  $\sigma$  if upon conjugating we obtain  $\sigma$ . One can then see that:

$$C_{S_5}(\sigma) = \{\iota, (1\ 2), (3\ 4), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\}$$

Again, not all of these are even, which leads to:

$$C_{A_5}(\sigma) = \{\iota, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

so:

$$|Cl(\sigma)| = |A_5|/|C_{S_5}(\sigma)| = 60/4 = 15$$

so once again, conjugacy classes of elements of cycle type  $(2, 2, 1, 1)$  will be the same in  $A_5$  as in  $S_5$ .

All in all, we get the following table relating conjugacy classes in  $S_5$  and  $A_5$ :

| <b>Cycle Type</b> | $ Cl_{S_5}(\sigma) $ | $ C_{S_5}(\sigma) $ | $ Cl_{A_5}(\sigma) $ | $ C_{A_5}(\sigma) $ |
|-------------------|----------------------|---------------------|----------------------|---------------------|
| 5                 | 24                   | 5                   | 12, 12               | 5                   |
| 3,1,1             | 20                   | 6                   | 20                   | 3                   |
| 2,2,1             | 15                   | 8                   | 15                   | 4                   |
| 1,1,1,1,1         | 1                    | 120                 | 1                    | 60                  |

Now, any normal subgroup of  $A_5$  will be a union of these conjugacy classes. As such we require that:

$$|N| = 1 + 12\alpha + 20\beta + 15\nu$$

where the values come from the order of the conjugacy classes, and  $\alpha \in [0, 1, 2], \beta, \nu \in [0, 1]$  (the identity element, which is the only elements in the conjugacy class of the identity must be in  $N$  for  $N$  to be a subgroup). We require that  $|N|$  divides  $|A_5| = 60 = 60 \times 1 = 30 \times 2 = 20 \times 3 = 15 \times 4 = 12 \times 5$ . Notice given this linear combination, the only possibilities are:

$$|N| = 1 \quad (\alpha = \beta = \nu = 0)$$

$$|N| = 60 \quad (\alpha = 2, \beta = \nu = 1)$$

Hence,  $N = \{\iota\}$  or  $N = A_5$ , and thus,  $A_5$  is simple. □

## 2.5 Simplicity of the Alternating Groups

### 2.5.1 Lemma: 3-Cycles are Conjugate in Alternating Groups

*If  $n \geq 5$  and  $\sigma, \sigma'$  are **3-cycles** in  $A_n$ , then  $\sigma, \sigma'$  are **conjugate** in  $A_n$ :*

$$\exists \tau \in A_n : \tau \sigma \tau^{-1} = \sigma'$$

*(Lemma 6.3.4)*

*Proof.* Assume  $\exists \tau \in S_n$ , where  $\tau$  is odd, such that  $\tau$  commutes with a 3-cycle  $\sigma$ :

$$\tau \sigma = \sigma \tau \implies \tau \sigma \tau^{-1} = \sigma$$

Now, let  $\nu$  be another odd permutation in  $S_n$ . Then  $\nu \tau$  will be an even permutation. Then:

$$(\nu \tau) \sigma (\nu \tau)^{-1} = \nu (\tau \sigma \tau^{-1}) \nu^{-1} = \nu \sigma \nu^{-1}$$

In other words, for any **odd** permutation  $\nu$ , we can find a corresponding even permutation  $\nu \tau$ , such that they conjugate  $\sigma$  to the same value. In other words, any 2 3-cycles, which will be conjugate in  $S_n$ , will also be conjugate in  $A_n$ , provided that there is an odd permutation with which they commute.

This is because of  $\sigma, \sigma'$  are conjugate in  $S_n$  then  $\exists \nu \in S_n$  such that:

$$\nu \sigma \nu^{-1} = \sigma'$$

If  $\nu$  is even, then  $\nu \in A_n$ , so  $\sigma, \sigma'$  are conjugate in  $A_n$ . Otherwise,  $\tau \nu \in A_n$ , so  $\sigma, \sigma'$  are still conjugate in  $A_n$ .

Now, let  $\sigma$  be a 3-cycle in  $S_n$ , where  $n \geq 5$ . Then trivially  $\sigma$  must leave at least 2 elements  $\alpha, \beta \in \{1, \dots, n\}$  **fixed**. Hence, if we define  $\tau = (\alpha \beta)$ ,  $\tau$  and  $\sigma$  will be disjoint, so in particular they must commute. Since  $\tau$  is a transposition, it is an odd permutation. Hence, by what we have just shown, 3-cycles are **conjugate** in  $A_n$ , as required. □

### 2.5.2 Lemma: 3-Cycles Generate Alternating Groups

*If  $n \geq 3$ , then  $A_n$  is generated by 3-cycles.  
(Lemma 6.3.5)*

*Proof.* Let  $\sigma \in A_n$ . Since  $\sigma$  is even, it can be written as an even number of transpositions. Then, it is sufficient to show that a product of 2 transpositions can be written as a single 3-cycle.

Consider 2 disjoint transpositions:

$$(a\ b)(c\ d) = (a\ c\ b)(c\ d\ a)$$

If the transpositions are not disjoint, without loss of generality we can assume that their first element is common:

$$(a\ b)(a\ c) = (a\ c\ b)$$

Since  $\sigma$  decomposes into an even number of transpositions, by the above we can write  $\sigma$  using 3-cycles (just group transpositions into pairs, and apply the transformations above), and so, any element in  $A_n$  can be decomposed into 3-cycles, as required. □

### 2.5.3 Lemma: Order of Fixed-Point-Free Subgroups

*We say  $\sigma \in S_n$  is **fixed-point-free** if:*

$$\forall i \in [1, n], \quad \sigma(i) \neq i$$

*Then, if  $H \leq S_n$ , and  $\forall \sigma \in H, \sigma \neq \iota$  such that  $\sigma$  is **fixed-point-free**,  
then  $|H| \leq n$ .  
(Lemma 6.3.6)*

### 2.5.4 Lemma: Order of Conjugacy Classes of Alternating Groups

*If  $n \geq 6$  and  $\sigma \in A_n$ , with  $\sigma \neq \iota$ , then:*

$$|Cl_{A_n}(\sigma)| \geq n$$

*(Lemma 6.3.7)*

*Intuitively this lemma says that conjugacy classes in  $A_n$  are **big**. For instance, the smallest non-trivial conjugacy class in  $A_6$  has 40 elements ( $A_6$  has 720 elements).*

### 2.5.5 Theorem: Alternating Groups are Simple When $n \geq 5$

$A_n$  is a **simple group** for  $n \geq 5$ .  
(Theorem 6.3.3)

*Proof.* We perform induction on  $n$ .

① **Base Case:**  $n = 5$

We already proved this!

② **Inductive Hypothesis:**  $n = k$

Assume this is true for  $n = k$ . That is,  $A_5, A_6, \dots, A_k$  are all simple groups.

③ **Inductive Step:**  $n = k + 1$

Consider the group  $A_{k+1}$ . Consider a normal subgroup:

$$H \triangleleft A_{k+1}$$

For  $i \in [1, k + 1]$  define the set  $B_i$  as the set of all even permutations which fix  $i$ :

$$B_i = \{\sigma \mid \sigma(i) = i, \quad \sigma \in A_n\}$$

We claim that:

$$B_i \cong A_k$$

This is simple to see:  $B_i$  is defined by fixing a unique element out of a set of  $k + 1$  total elements; in other words, it permutes all the other  $k$  elements, whilst keeping  $i$  fixed. This is the definition of a permutation group of  $k$  elements. Since  $B_i$  only contains even permutations, it must be isomorphic to  $A_k$ .

Moreover, recall the Second Isomorphism Theorem:

Let  $N \triangleleft G$  and  $H \leq G$ . Then:

1.  $HN \leq G$
2.  $N \triangleleft HN$
3.  $H \cap N \triangleleft H$
4. there exists an isomorphism:

$$H/(H \cap N) \cong HN/N$$

(Theorem 2.3.7)

so since  $H \triangleleft A_k$  and  $B_i \leq A_k$ :

$$H \cap B_i \triangleleft B_i$$

Since  $B_i \cong A_k$ , and  $A_k$  is a simple group by inductive hypothesis, it follows that  $B_i$  is simple, so:

$$H \cap B_i = B_i \quad H \cap B_i = \iota$$

First, assume that:

$$H \cap B_i = B_i$$

This is true **if and only if**  $B_i \subseteq H$ . Now, since  $B_i \cong A_k \subset A_{k+1}$ , we know that  $B_i$  contains at least one 3-cycle (since 3-cycles are even permutations), and so,  $H$  contains a 3-cycle.

But  $H$  is a normal subgroup of  $A_{k+1}$ , and normal subgroups are unions of conjugacy classes. As such,  $H$  must contain the **whole** conjugacy class of 3-cycles in  $A_{k+1}$ . But then, since  $A_{k+1}$  is an alternating group, it is generated by 3-cycles. Since  $H$  contains all the 3-cycles which generate  $A_{k+1}$ , it must be the case that  $A_{k+1} \subseteq H$ . Hence, it follows that  $H = A_{k+1}$ .

Secondly, assume that:

$$H \cap B_i = \iota$$

In other words, if  $\sigma \in H$ , then  $\sigma$  fixes no element in  $i \in [1, n]$ . But then,  $H$  is a **fixed-point-free** subgroup of  $S_{k+1}$ , so:

$$H \leq k + 1$$

Now take some  $\sigma \in H$  such that  $\sigma \neq \iota$ . We also have that:

$$|Cl_{A_{k+1}}(\sigma)| \geq k + 1$$

But then, recall  $Cl_{A_{k+1}}(\sigma)$  won't contain the identity, so:

$$Cl_{A_{k+1}}(\sigma) \cup \{\iota\} \subset H$$

which implies:

$$|H| \geq (k + 1) + 1$$

This is a contradiction, and so, no such non-identity must exist. Hence,  $\sigma = \iota$  is the only possible element in  $H$ , and so,  $A_{k+1}$  must be simple.

□