Simplicity of A_5

GU4041

Columbia University

April 11, 2020

The alternating group A_5 is simple

Theorem

The alternating group $A_5 \subset S_5$ is a simple group of order 60.

In fact we have the general theorem:

Theorem

For any $n \geq 5$, the alternating group $A_n \subset S_n$ is a simple group of order $\frac{n!}{2}$.

The alternating group A_5 is simple

Theorem

The alternating group $A_5 \subset S_5$ is a simple group of order 60.

In fact we have the general theorem:

Theorem

For any $n \geq 5$, the alternating group $A_n \subset S_n$ is a simple group of order $\frac{n!}{2}$.

The conjugacy classes in S_5 are determined by their cycle decomposition, The partitions of 5 are

- $5 = 5$; a 5-cycle is the product of 4 transpositions, hence is even.
- $5 = 4 + 1$; a 4-cycle is the product of 3 transpositions, hence is odd.
- $5 = 3 + 2$; a 3-cycle is the product of 2 transpositions, hence its product with a disjoint transposition is odd.
- $5 = 3 + 1 + 1$; a 3-cycle is even.
- $5 = 2 + 2 + 1$; an even product of two disjoint 2-cycles.
- $5 = 2 + 1 + 1 + 1$; a 2-cycle is odd.
- $5 = 1 + 1 + 1 + 1 + 1$; the identity is even.

Conjugacy classes in S_5

The conjugacy classes in S_5 are determined by their cycle decomposition, The partitions of 5 are

- $5 = 5$; a 5-cycle is the product of 4 transpositions, hence is even.
- $5 = 4 + 1$; a 4-cycle is the product of 3 transpositions, hence is odd.
- $5 = 3 + 2$; a 3-cycle is the product of 2 transpositions, hence its product with a disjoint transposition is odd.
- $5 = 3 + 1 + 1$; a 3-cycle is even.
- $5 = 2 + 2 + 1$; an even product of two disjoint 2-cycles.
- $5 = 2 + 1 + 1 + 1$; a 2-cycle is odd.
- $5 = 1 + 1 + 1 + 1 + 1$; the identity is even.

Conjugacy classes in S_5

The conjugacy classes in S_5 are determined by their cycle decomposition, The partitions of 5 are

- $5 = 5$; a 5-cycle is the product of 4 transpositions, hence is even.
- $5 = 4 + 1$; a 4-cycle is the product of 3 transpositions, hence is odd.
- $5 = 3 + 2$; a 3-cycle is the product of 2 transpositions, hence its product with a disjoint transposition is odd.
- $5 = 3 + 1 + 1$; a 3-cycle is even.
- $5 = 2 + 2 + 1$; an even product of two disjoint 2-cycles.
- $5 = 2 + 1 + 1 + 1$; a 2-cycle is odd.
- $5 = 1 + 1 + 1 + 1 + 1$; the identity is even.

Conjugacy classes in S_5

The conjugacy classes in S_5 are determined by their cycle decomposition, The partitions of 5 are

- $5 = 5$; a 5-cycle is the product of 4 transpositions, hence is even.
- $5 = 4 + 1$; a 4-cycle is the product of 3 transpositions, hence is odd.
- $5 = 3 + 2$; a 3-cycle is the product of 2 transpositions, hence its product with a disjoint transposition is odd.
- $5 = 3 + 1 + 1$; a 3-cycle is even.
- $5 = 2 + 2 + 1$; an even product of two disjoint 2-cycles.
- $5 = 2 + 1 + 1 + 1$; a 2-cycle is odd.
- $5 = 1 + 1 + 1 + 1 + 1$; the identity is even.

Conjugacy classes in S_5

The conjugacy classes in S_5 are determined by their cycle decomposition, The partitions of 5 are

- $5 = 5$; a 5-cycle is the product of 4 transpositions, hence is even.
- $5 = 4 + 1$; a 4-cycle is the product of 3 transpositions, hence is odd.
- $5 = 3 + 2$; a 3-cycle is the product of 2 transpositions, hence its product with a disjoint transposition is odd.
- $5 = 3 + 1 + 1$; a 3-cycle is even.
- $5 = 2 + 2 + 1$; an even product of two disjoint 2-cycles.
- $5 = 2 + 1 + 1 + 1$; a 2-cycle is odd.
- $5 = 1 + 1 + 1 + 1 + 1$; the identity is even.

Conjugacy classes in S_5

The conjugacy classes in S_5 are determined by their cycle decomposition, The partitions of 5 are

- $5 = 5$; a 5-cycle is the product of 4 transpositions, hence is even.
- $5 = 4 + 1$; a 4-cycle is the product of 3 transpositions, hence is odd.
- $5 = 3 + 2$; a 3-cycle is the product of 2 transpositions, hence its product with a disjoint transposition is odd.
- $5 = 3 + 1 + 1$; a 3-cycle is even.
- $5 = 2 + 2 + 1$; an even product of two disjoint 2-cycles.
- $5 = 2 + 1 + 1 + 1$; a 2-cycle is odd.
- $5 = 1 + 1 + 1 + 1 + 1$; the identity is even.

Conjugacy classes in S_5

The conjugacy classes in S_5 are determined by their cycle decomposition, The partitions of 5 are

- $5 = 5$; a 5-cycle is the product of 4 transpositions, hence is even.
- $5 = 4 + 1$; a 4-cycle is the product of 3 transpositions, hence is odd.
- $5 = 3 + 2$; a 3-cycle is the product of 2 transpositions, hence its product with a disjoint transposition is odd.
- $5 = 3 + 1 + 1$; a 3-cycle is even.
- $5 = 2 + 2 + 1$; an even product of two disjoint 2-cycles.
- $5 = 2 + 1 + 1 + 1$; a 2-cycle is odd.
- $5 = 1 + 1 + 1 + 1 + 1$; the identity is even.

Conjugacy classes in S_5

The conjugacy classes in S_5 are determined by their cycle decomposition, The partitions of 5 are

- $5 = 5$; a 5-cycle is the product of 4 transpositions, hence is even.
- $5 = 4 + 1$; a 4-cycle is the product of 3 transpositions, hence is odd.
- $5 = 3 + 2$; a 3-cycle is the product of 2 transpositions, hence its product with a disjoint transposition is odd.
- $5 = 3 + 1 + 1$; a 3-cycle is even.
- $5 = 2 + 2 + 1$; an even product of two disjoint 2-cycles.
- $5 = 2 + 1 + 1 + 1$; a 2-cycle is odd.
- $5 = 1 + 1 + 1 + 1 + 1$; the identity is even.

Conjugacy classes in A_5

There are thus 4 S_5-conjugacy classes contained in A_5:

- $5 = 5$, with $4! = 24$ elements (fix the first one, then the next four can be chosen freely).
- $5 = 3 + 1 + 1$; with $\binom{5}{3} = 10$ triples, plus their inverses, for 20 elements
- $5 = 2 + 2 + 1$; with 5 choices of the fixed element, $\times \binom{4}{2} = 6$, for 30 pairs $(ab)(cd)$, divided by 2 because $(ab)(cd) = (cd)(ab)$, to give 15 elements.
- $5 = 1 + 1 + 1 + 1 + 1$ for 1 identity element

And $24 + 20 + 15 + 1 = 60 = |A_5|$. But the S_5-orbit of an element of A_5 may be bigger than its A_5 orbit!

Conjugacy classes in A_5

There are thus 4 S_5-conjugacy classes contained in A_5:

- $5 = 5$, with $4! = 24$ elements (fix the first one, then the next four can be chosen freely).
- $5 = 3 + 1 + 1$; with $\binom{5}{3} = 10$ triples, plus their inverses, for 20 elements
- $5 = 2 + 2 + 1$; with 5 choices of the fixed element, $\times \binom{4}{2} = 6$, for 30 pairs $(ab)(cd)$, divided by 2 because $(ab)(cd) = (cd)(ab)$, to give 15 elements.
- $5 = 1 + 1 + 1 + 1 + 1$ for 1 identity element

And $24 + 20 + 15 + 1 = 60 = |A_5|$. But the S_5-orbit of an element of A_5 may be bigger than its A_5 orbit!

Conjugacy classes in A_5

There are thus 4 S_5-conjugacy classes contained in A_5:

- $5 = 5$, with $4! = 24$ elements (fix the first one, then the next four can be chosen freely).
- $5 = 3 + 1 + 1$; with $\binom{5}{3} = 10$ triples, plus their inverses, for 20 elements
- $5 = 2 + 2 + 1$; with 5 choices of the fixed element, $\times \binom{4}{2} = 6$, for 30 pairs $(ab)(cd)$, divided by 2 because $(ab)(cd) = (cd)(ab)$, to give 15 elements.
- $5 = 1 + 1 + 1 + 1 + 1$ for 1 identity element

And $24 + 20 + 15 + 1 = 60 = |A_5|$. But the S_5-orbit of an element of A_5 may be bigger than its A_5 orbit!

Conjugacy classes in A_5

There are thus 4 S_5-conjugacy classes contained in A_5:

- $5 = 5$, with $4! = 24$ elements (fix the first one, then the next four can be chosen freely).
- $5 = 3 + 1 + 1$; with $\binom{5}{3} = 10$ triples, plus their inverses, for 20 elements
- $5 = 2 + 2 + 1$; with 5 choices of the fixed element, $\times \binom{4}{2} = 6$, for 30 pairs $(ab)(cd)$, divided by 2 because $(ab)(cd) = (cd)(ab)$, to give 15 elements.
- $5 = 1 + 1 + 1 + 1 + 1$ for 1 identity element

And $24 + 20 + 15 + 1 = 60 = |A_5|$. But the S_5-orbit of an element of A_5 may be bigger than its A_5 orbit!

Conjugacy classes in A_5

There are thus 4 S_5-conjugacy classes contained in A_5:

- $5 = 5$, with $4! = 24$ elements (fix the first one, then the next four can be chosen freely).
- $5 = 3 + 1 + 1$; with $\binom{5}{3} = 10$ triples, plus their inverses, for 20 elements
- $5 = 2 + 2 + 1$; with 5 choices of the fixed element, $\times \binom{4}{2} = 6$, for 30 pairs $(ab)(cd)$, divided by 2 because $(ab)(cd) = (cd)(ab)$, to give 15 elements.
- $5 = 1 + 1 + 1 + 1 + 1$ for 1 identity element

And $24 + 20 + 15 + 1 = 60 = |A_5|$. But the S_5-orbit of an element of A_5 may be bigger than its A_5 orbit!

Conjugacy classes in A_5

There are thus 4 S_5-conjugacy classes contained in A_5:

- $5 = 5$, with $4! = 24$ elements (fix the first one, then the next four can be chosen freely).
- $5 = 3 + 1 + 1$; with $\binom{5}{3} = 10$ triples, plus their inverses, for 20 elements
- $5 = 2 + 2 + 1$; with 5 choices of the fixed element, $\times \binom{4}{2} = 6$, for 30 pairs $(ab)(cd)$, divided by 2 because $(ab)(cd) = (cd)(ab)$, to give 15 elements.
- $5 = 1 + 1 + 1 + 1 + 1$ for 1 identity element

And $24 + 20 + 15 + 1 = 60 = |A_5|$. But the S_5-orbit of an element of A_5 may be bigger than its A_5 orbit!

Conjugacy classes in A_5

More precisely, let $g \in A_5$, with centralizer $C_g \subset S_5$, $C'_g \in A_5$. So Then the conjugacy class $[g] \subset S_5$ has order $|S_5|/|C_g|$, the A_5-conjugacy class $[g]' \subset A_5$ has order $|A_5|/|C_g|$. In particular, $|[g]'$ must divide $60 = |A_5|$. This shows that not all 5 cycles are conjugate in A_5.

Lemma

Let $g \in A_5$. Then its conjugacy class $[g]$ in S_5 is the union of either 1 or 2 conjugacy classes in A_5; if there are 2 then they are both of the same size.

More precisely, let $g \in A_5$, with centralizer $C_g \subset S_5$, $C'_g \in A_5$. So Then the conjugacy class $[g] \subset S_5$ has order $|S_5|/|C_g|$, the A_5-conjugacy class $[g]' \subset A_5$ has order $|A_5|/|C_g|$. In particular, $|[g]'$ must divide $60 = |A_5|$. This shows that not all 5 cycles are conjugate in A_5.

Lemma

Let $g \in A_5$. Then its conjugacy class $[g]$ in S_5 is the union of either 1 or 2 conjugacy classes in A_5; if there are 2 then they are both of the same size.

More precisely, let $g \in A_5$, with centralizer $C_g \subset S_5$, $C'_g \in A_5$. So Then the conjugacy class $[g] \subset S_5$ has order $|S_5|/|C_g|$, the A_5-conjugacy class $[g]' \subset A_5$ has order $|A_5|/|C_g|$. In particular, $|[g]'$ must divide $60 = |A_5|$. This shows that not all 5 cycles are conjugate in A_5.

Lemma

Let $g \in A_5$. Then its conjugacy class $[g]$ in S_5 is the union of either 1 or 2 conjugacy classes in A_5; if there are 2 then they are both of the same size.

Conjugacy classes in A_5

Corollary

There are two conjugacy classes of 5-cycles in A_5, and one conjugacy class of products of disjoint 2-cycles.

Proof of corollary: Since 24 does not divide 60, the 5 cycles form more than 1, thus 2 conjugacy classes; but 15 is not even, so it is a single conjugacy class.

Conjugacy classes in A_5

Corollary

There are two conjugacy classes of 5-cycles in A_5, and one conjugacy class of products of disjoint 2-cycles.

Proof of corollary: Since 24 does not divide 60, the 5 cycles form more than 1, thus 2 conjugacy classes; but 15 is not even, so it is a single conjugacy class.

We can now prove that A_5 is simple. Let $N \subset A_5$ be a normal subgroup. It is the union of conjugacy classes, and its order divides 60, and it must contain the identity. The partition of 60 into the orders of conjugacy classes is either

$$60 = 1 + 12 + 12 + 15 + 20$$

(which is in fact correct) or

$$60 = 1 + 12 + 12 + 15 + 10 + 10.$$

The proper divisors of 60 bigger than 10 are 12, 15, 20, 30. No partial sum of these partitions adds up to one of these divisors. So the only possible N are A_5 and the identity.

We can now prove that A_5 is simple. Let $N \subset A_5$ be a normal subgroup. It is the union of conjugacy classes, and its order divides 60, and it must contain the identity. The partition of 60 into the orders of conjugacy classes is either

$$60 = 1 + 12 + 12 + 15 + 20$$

(which is in fact correct) or

$$60 = 1 + 12 + 12 + 15 + 10 + 10.$$

The proper divisors of 60 bigger than 10 are 12, 15, 20, 30. No partial sum of these partitions adds up to one of these divisors. So the only possible N are A_5 and the identity.

We can now prove that A_5 is simple. Let $N \subset A_5$ be a normal subgroup. It is the union of conjugacy classes, and its order divides 60, and it must contain the identity. The partition of 60 into the orders of conjugacy classes is either

$$60 = 1 + 12 + 12 + 15 + 20$$

(which is in fact correct) or

$$60 = 1 + 12 + 12 + 15 + 10 + 10.$$

The proper divisors of 60 bigger than 10 are 12, 15, 20, 30. No partial sum of these partitions adds up to one of these divisors. So the only possible N are A_5 and the identity.

Simplicity of A_5

We can now prove that A_5 is simple. Let $N \subset A_5$ be a normal subgroup. It is the union of conjugacy classes, and its order divides 60, and it must contain the identity. The partition of 60 into the orders of conjugacy classes is either

$$60 = 1 + 12 + 12 + 15 + 20$$

(which is in fact correct) or

$$60 = 1 + 12 + 12 + 15 + 10 + 10.$$

The proper divisors of 60 bigger than 10 are 12, 15, 20, 30. No partial sum of these partitions adds up to one of these divisors. So the only possible N are A_5 and the identity.

Proof of the Lemma

Let X be the set of A_5 conjugacy classes contained in $[g]$. We let S_5 act on X by conjugation: clearly $[h]' \subset [g]$ if and only h is conjugate to g in S_5. Moreover, the action of S_5 on X is transitive, by definition. The stabilizer $S_{[g]'} \subset S_5$ contains A_5, again by definition. Thus either $S_{[g]'} = A_5$ or $S_{[g]'} = S_5$.

If $S_{[g]'} = S_5$ then $[g]' = [g]$, and $[g]$ contains only one A_5-conjugacy class. Otherwise, $[g] = [g]' \coprod [h]'$ for some $h = sgs^{-1}$, $s \in S_5 \setminus A_5$.

Proof of the Lemma

Let X be the set of A_5 conjugacy classes contained in $[g]$. We let S_5 act on X by conjugation: clearly $[h]' \subset [g]$ if and only h is conjugate to g in S_5. Moreover, the action of S_5 on X is transitive, by definition. The stabilizer $S_{[g]'} \subset S_5$ contains A_5, again by definition. Thus either $S_{[g]'} = A_5$ or $S_{[g]'} = S_5$.

If $S_{[g]'} = S_5$ then $[g]' = [g]$, and $[g]$ contains only one A_5-conjugacy class. Otherwise, $[g] = [g]' \coprod [h]'$ for some $h = sgs^{-1}$, $s \in S_5 \setminus A_5$.

Proof of the Lemma

Let X be the set of A_5 conjugacy classes contained in $[g]$. We let S_5 act on X by conjugation: clearly $[h]' \subset [g]$ if and only h is conjugate to g in S_5. Moreover, the action of S_5 on X is transitive, by definition. The stabilizer $S_{[g]'} \subset S_5$ contains A_5, again by definition. Thus either $S_{[g]'} = A_5$ or $S_{[g]'} = S_5$.
If $S_{[g]'} = S_5$ then $[g]' = [g]$, and $[g]$ contains only one A_5-conjugacy class. Otherwise, $[g] = [g]' \coprod [h]'$ for some $h = sgs^{-1}$, $s \in S_5 \setminus A_5$.

Proof of the Lemma

Let X be the set of A_5 conjugacy classes contained in $[g]$. We let S_5 act on X by conjugation: clearly $[h]' \subset [g]$ if and only h is conjugate to g in S_5. Moreover, the action of S_5 on X is transitive, by definition. The stabilizer $S_{[g]'} \subset S_5$ contains A_5, again by definition. Thus either $S_{[g]'} = A_5$ or $S_{[g]'} = S_5$.
If $S_{[g]'} = S_5$ then $[g]' = [g]$, and $[g]$ contains only one A_5-conjugacy class. Otherwise, $[g] = [g]' \coprod [h]'$ for some $h = sgs^{-1}$, $s \in S_5 \setminus A_5$.

Proof of the Lemma, concluded

It remains to show that

$$|[h]'| = |[sgs^{-1}]'| = |[g]'|,$$

in other words, that

$$s : [g]' \to [h]'; aga^{-1} \mapsto s(aga^{-1})s^{-1} = (sas^{-1})sgs^{-1}(sas^{-1})^{-1}$$

is a bijection.
But conjugation by s^{-1} is the inverse bijection, so we are done.

Proof of the Lemma, concluded

It remains to show that

$$|[h]'| = |[sgs^{-1}]'| = |[g]'|,$$

in other words, that

$$s : [g]' \to [h]'; aga^{-1} \mapsto s(aga^{-1})s^{-1} = (sas^{-1})sgs^{-1}(sas^{-1})^{-1}$$

is a bijection.
But conjugation by s^{-1} is the inverse bijection, so we are done.