

# $A_n$ is simple

Patrick J. Morandi

In this note we will prove that  $A_n$  is simple if  $n \geq 5$ , by first proving that  $A_5$  is simple, and then giving an induction argument for  $A_n$  for  $n \geq 5$ . The simplicity of  $A_5$  is enough to prove that  $S_n$  is not a solvable group for all  $n \geq 5$ . The proof we give of the simplicity of  $A_5$  uses the idea of conjugacy classes. The idea of the proof is that given a normal subgroup of  $A_5$ , the subgroup is a union of some of the conjugacy classes of  $A_5$  from the normality assumption. If we can show that no union of conjugacy classes (other than  $\{e\}$  and  $A_5$ ) can be a subgroup of  $A_5$ , we will have proved that  $A_5$  contains no nontrivial normal subgroup.

We review now some of the notions behind the idea of conjugacy. If  $G$  is a group, then  $G$  acts on itself by conjugation. If  $x \in G$ , then the orbit of  $x$  under this action is the conjugacy class  $\mathcal{O}_x = \{gxg^{-1} : g \in G\}$ . We also have the isotropy group  $G_x = \{g \in G : gxg^{-1} = x\}$ . Note that this group is also the centralizer  $C(x)$  of  $x$ ; it consists of the elements of  $G$  that commute with  $x$ . Recall a basic fact of group actions of a finite group: if  $G$  acts on a set  $X$ , we can define the orbit  $\mathcal{O}_x$  of an  $x \in X$  and the isotropy group  $G_x = \{g \in G : gx = x\}$ , and their sizes are related by the equation  $|\mathcal{O}_x| = [G : G_x]$ . So, in this example of conjugation, we have  $|\mathcal{O}_x| = [G : C(x)]$  for all  $x \in G$ .

Now consider  $S_5$ . It is known that in  $S_n$  for any  $n$ , the conjugacy class of an element is the set of all elements of the same cycle structure. The possible cycle structures of elements of  $S_5$  are listed in the following table.

cycle structure	representative element	number of elements
5-cycle	(12345)	24
4-cycle	(1234)	30
3-cycle	(123)	20
2-cycle	(12)	10
1-cycle	$e$	1
3-cycle · 2-cycle	(123)(45)	20
2-cycle · 2-cycle	(12)(34)	15

We are interested in the conjugacy classes of  $A_5$ . If  $x \in A_5$ , then the conjugacy class of  $x$  is  $\{gxg^{-1} : g \in A_5\}$ , while the conjugacy class of  $x$  in  $S_5$  is  $\{gxg^{-1} : g \in S_5\}$ . So, the conjugacy class of  $x$  in  $A_5$  could conceivably be smaller than its conjugacy class in  $S_5$ .

We now determine the conjugacy classes for  $A_5$ . In order to determine the sizes of these classes, we need to determine the order of the centralizer in  $A_5$  of an element  $x \in A_5$ . We do this by making use of the corresponding information for  $S_5$ . To distinguish between conjugacy classes in  $S_5$  and in  $A_5$ , we will write  $\mathcal{O}_{x,S_5}$  for the conjugacy class of  $x$  in  $S_5$ , and  $\mathcal{O}_x$  for the conjugacy class in  $A_5$ . Similarly,  $C_{S_5}(x)$  will denote the centralizer of  $x$  in  $S_5$ , while we denote by  $C(x)$  the centralizer of  $x$  in  $A_5$ .

First, note that  $A_5$  consists of the 5-cycles, the 3-cycles, the product of 2 disjoint 2-cycles, and  $e$ . It is clear that the conjugacy class of  $e$  is  $\{e\}$ . For the product of disjoint 2-cycles, consider  $x = (12)(34)$ . In  $S_5$ , we have  $|\mathcal{O}_{x,S_5}| = 15 = 120/|C_{S_5}(x)|$ , so  $|C_{S_5}(x)| = 8$ . We can determine  $C_{S_5}(x)$  by producing elements that commute with  $x$ , and when we have 8 we will have all of  $C_{S_5}(x)$ . By a little trial and error, we obtain  $C_{S_5}(x) = \langle (1324), (13)(24) \rangle$ . Moreover  $C(x) = C_{S_5}(x) \cap A_5 = \{e, (12)(34), (13)(24), (14)(23)\}$ . So, the centralizer of  $x$  in  $A_5$  has order 4. Therefore,  $|\mathcal{O}_x| = [A_5 : C(x)] = 60/4 = 15$ . Thus, the entire conjugacy class of  $x$  in  $S_5$  is the conjugacy class of  $x$  in  $A_5$ .

Now consider  $x = (123)$ . We have  $|\mathcal{O}_{x,S_5}| = 20$ , so  $|C_{S_5}(x)| = 6$ . Again, by trial and error, we see that  $C_{S_5}(x) = \langle (123), (45) \rangle$ , So  $C(x) = \langle (123) \rangle$ . So,  $|\mathcal{O}_x| = 60/3 = 20$ , and, again, this implies that  $\mathcal{O}_x = \mathcal{O}_{x,S_5}$ . Finally, for  $x = (12345)$ , we have  $|C_{S_5}(x)| = |S_5|/|\mathcal{O}_{x,S_5}| = 120/24 = 5$ . This forces  $C_{S_5}(x) = \langle (12345) \rangle$ , and so  $C(x) = \langle (12345) \rangle$ . Thus,  $|\mathcal{O}_x| = 60/5 = 12$ . Therefore, the conjugacy class of  $(12345)$  consists of just 12 of the 24 5-cycles. Since this argument works for any 5-cycle, if we let  $x$  be any 5-cycle not in the conjugacy class of  $(12345)$ , then the conjugacy class of  $x$  will consist of the other 12 5-cycles. Thus, the conjugacy class of a 5-cycle in  $S_5$  is the union of two conjugacy classes in  $A_5$ .

We have shown that there are 5 conjugacy classes of  $A_5$ , and their sizes are 1, 12, 12, 15, and 20. We can now prove the main result of this note.

**Theorem 1** *The group  $A_5$  is simple.*

**Proof.** Let  $N$  be a normal subgroup of  $A_5$ . Then it is a union of some of the conjugacy classes of  $A_5$ . However, the order of  $N$  must divide 60. A short calculation will show that no union of some of these conjugacy classes that includes  $\{e\}$  has order a divisor of 60, unless the union is  $\{e\}$  or  $A_5$ . Thus,  $A_5$  is simple. ■

Recall that a subgroup of a solvable group is solvable, and that a simple non-Abelian group is not solvable. Since  $A_5$  is isomorphic to a subgroup of  $S_n$  for each  $n \geq 5$ , we get the following corollary.

**Corollary 2** *If  $n \geq 5$ , then  $S_n$  is not a solvable group.*

With the result about  $A_5$  and induction, we can prove that  $A_n$  is simple for each  $n \geq 5$ .

**Theorem 3** *If  $n \geq 5$ , then  $A_n$  is a simple group.*

**Proof.** We prove this by induction on  $n$ ; the case  $n = 5$  is already done. So, suppose that  $n \geq 6$ , and that  $A_{n-1}$  is simple. For each  $i \leq n$ , let  $G_i = \{\sigma \in A_n : \sigma(i) = i\}$ . Then  $G_i$  is a subgroup of  $A_n$  isomorphic to  $A_{n-1}$ . So,  $G_i$  is simple by induction. Moreover, if  $\sigma_i \in A_n$  is any element with  $\sigma_i(j) = i$  (possible since  $A_n$  is a transitive subgroup of  $S_n$ ), then  $G_i = \sigma_i G_j \sigma_i^{-1}$ . Thus, any two of the  $G_i$  are conjugate in  $A_n$ . Let  $N$  be a normal subgroup of  $A_n$ . Then  $N \cap G_i = \{e\}$  or  $N \cap G_i = G_i$ . If  $N \cap G_i = G_i$  for some  $i$ , then in fact  $N \cap G_j = G_j$  for all  $j$ , since  $G_j$  is conjugate to  $G_i$  for each  $j$ . So since  $N$  is normal, if  $N$  contains  $G_i$  for some  $i$ , it contains all of them. But, since  $n \geq 6$ , any product of two transpositions is in  $G_i$  for some  $i$ , and any element of  $A_n$  is a product of such permutations. So,  $N = A_n$ .

On the other hand, if  $N \cap G_i = \{e\}$  for each  $i$ , then each element of  $N$  fixes no integer. Consequently, if  $\sigma, \tau \in N$  with  $\sigma(i) = \tau(i)$  for some  $i$ , then  $\sigma^{-1}\tau(i) = i$ , so  $\sigma^{-1}\tau \in N \cap G_i = \{e\}$ . This forces  $\sigma = \tau$ . So, distinct elements of  $N$  never agree at any integer. Consider some  $\sigma \in N$ , and write  $\sigma$  as a product of disjoint cycles, say  $\sigma = c_1 \cdots c_t$  with  $c_i$  an  $r_i$ -cycle (and  $r_1 \geq r_2 \geq \cdots \geq r_t$ ). if  $r_1 \geq 3$ , say  $c_1 = (i_1 \cdots i_r)$ . Let  $\rho = (i_3 j k)$ , with  $j, k \notin \{i_1, i_2, i_3\}$ ; it is possible to do this since  $n \geq 6$ . Let  $\tau = \rho \sigma \rho^{-1} \in N$ . Both  $\sigma$  and  $\tau$  send  $i_1$  to  $i_2$  but  $\sigma \neq \tau$  since  $\sigma(i_2) = i_3$  and  $\tau(i_2) = j$ , a contradiction. So, any  $\sigma \in N$  is a product of transpositions. Now suppose  $\sigma = (ij)(kl) \cdots \in N$ . Let  $\rho = (lpq)$  with  $p, q \notin \{i, j, k, l\}$ ; again, this is possible since  $n \geq 6$ . Then if  $\tau = \rho \sigma \rho^{-1}$ , both  $\sigma$  and  $\tau$  send  $i$  to  $j$ , but  $\sigma(k) = l$  while  $\tau(k) = p$ , a contradiction. So, in this case we must have  $N = \{e\}$ . Thus, we have proven that either  $N = A_n$  or  $N = \{e\}$ . That is,  $A_n$  is simple. ■