

### Simplicity of $A_n$ ( $n \geq 5$ ).

LEMMA 1. *If  $n \geq 3$  then any proper normal subgroup of the alternating group  $A_n$  has index divisible by 3.*

*Proof.* Let  $p = |A_n/H|$ . Then every  $p$ -th power in  $A_n$  lies in  $H$ . So if  $p$  is not divisible by 3 then every 3-cycle lies in  $H$ , whence  $H = A_n$ . (Any 3-cycle  $c$  satisfies  $c = c^{3n+1} = (c^{-1})^{3n+2}$ , for any integer  $n$ .)

LEMMA 2.  *$A_5$  is simple.*

*Proof.* By Lemma 1, any proper  $H \triangleleft A_5$  has order dividing 20. So  $H$  cannot contain any order-3 element, i.e., 3-cycle; and also  $H$  cannot contain any 5-cycle, since any such has 6 conjugates, and 6 doesn't divide 20. The only remaining nontrivial even permutations are the 15 products  $(ab)(cd)$  of two disjoint 2-cycles, any two of which are conjugate in  $S_5$ , hence in  $A_5$  (since 15 is odd); and since 15 doesn't divide 20, these can't be in  $H$  either. Thus  $|H| = 1$ .

THEOREM.  *$A_n$  is simple for  $n \geq 5$ .*

*Proof.* Proceed by induction, the case  $n = 5$  being given above. So suppose  $n > 5$ ,  $A_{n-1}$  is simple, and  $H \triangleleft A_n$ . Then  $H \cap A_{n-1}$ , being normal in  $A_{n-1}$ , is either  $A_{n-1}$  or trivial.

In the former case, any 3-cycle, being conjugate to one in  $A_{n-1}$ , lies in  $H$ , making  $H = A_n$ . The same holds if  $H$  contains any conjugate of  $A_{n-1}$ .

The remaining possibility is that  $H$  intersects any conjugate of  $A_{n-1}$  trivially, i.e., no nonidentity permutation  $h \in H$  has a fixed point. Writing  $h$  and its powers (none of which have fixed points) as products of cycles, one sees then that  $h$  is a product of  $p$   $q$ -cycles for some  $p$  and  $q$  such that  $pq = n$ . Any element in the centralizer  $C_h$  of  $h$  produces a permutation of these cycles, and thus there is a surjective homomorphism  $C_h \rightarrow S_p$ . The kernel consists of all elements that are products of powers of these cycles, and so has cardinality  $q^p$ . Thus  $|C_h| = (q^p)(p!)$ , whence the number of  $S_n$ -conjugates of  $h$  is  $n!/(q^p)(p!)$ . The number of  $A_n$ -conjugates is at least half of that, and—since all such conjugates lie in  $H$ —must be less than

$$|H| = |H|/|H \cap A_{n-1}| < |A_n|/|A_{n-1}| = n.$$

Now  $n!/(q^p)(p!)$  is the product of all numbers  $< n$  which are not multiples of  $q$ , which product is at least  $(n-1)(n-2)$  if  $q > 2$ , or  $(n-1)(n-3)$  if  $q = 2$ . In either case, since  $(n-1)(n-2)/2 > (n-1)(n-3)/2 > n$  when  $n > 5$ , we must have  $q = 1$ . Thus  $|H| = 1$ .  $\square$

For another proof, see Clark, §83.