

## Notes on the simplicity of $A_n$

Felix Lazebnik

October 5, 2016

We begin with several preliminary results. The image of a point  $x \in [n]$  under a permutation  $\pi \in S_n$  is denoted by  $\pi(x)$ , and for any two permutations  $\pi, \sigma \in S_n$ ,  $(\pi\sigma)(x) = \pi(\sigma(x))$ .

**Proposition 1.** *Let  $i, j, k, l$  be distinct element of  $[n]$ ,  $n \geq 4$ . Then*

$$(ij)(ik) = (ikj) \quad \text{and} \quad (il)(jk) = (ilj)(jkl).$$

*Proof.* Just look at the images of the elements  $\{i, j, k, l\}$  in these permutations, and show that any other element of  $[n]$  is fixed by the permutations.  $\square$

**Proposition 2.** *Every 3-cycle  $(ijk)$  is an even permutation, and  $A_n$  is generated by all 3-cycles.*

*Proof.* As  $(ikj) = (ij)(ik)$ , the first statement is proven. Let  $\pi \in A_n$ . Then  $\pi = \tau_1\tau_2 \cdots \tau_{2k}$  for some transpositions  $\tau_m$ . Then

$$\pi = (\tau_1\tau_2)(\tau_3\tau_4) \cdots (\tau_{2k-1}\tau_{2k}).$$

By Proposition 1, each  $\tau_{2m-1}\tau_{2m}$  is a 3-cycle or a product of two 3-cycles.  $\square$

**Theorem 1.** (Galois) *Let  $A_n$  be the alternating group on  $[n]$ ,  $n \geq 1$ . Then  $A_n$  is simple if  $n \neq 4$ .*

*Proof.* It is obvious that  $A_1$ ,  $A_2$  and  $A_3$  are simple.  $A_4$  is of order 12, and it contains the Klein group  $\{e, (12)(34), (13)(24), (14)(23)\}$  of order 4 which is normal in  $A_4$  (as the union of two conjugate classes).

Therefore we may assume that  $n \geq 5$ . Let  $\langle e \rangle \neq N$ , and  $N$  be a *normal* subgroup of  $A_n$ . We want to show that  $N = A_n$ .

The main idea is to prove that  $N$  contains all 3-cycles, and the statement will follow from Proposition 2. In order to do this, we first show that if  $N$  contains a 3-cycle, then it contains them all. That will be easy. After that we show that  $N$  contains a 3-cycle. This will be hard.

**Lemma 1.** *If  $N$  contains at least one 3-cycle, it contains all 3-cycles. For all  $n \geq 5$ , any two 3-cycles are conjugate in  $A_n$ .*

*Proof.* The fact that any 3-cycles are conjugate in  $S_n$  for any  $n \geq 3$  was proven before. Let  $\sigma = (a_1a_2a_3) \in N$ , and  $\gamma = (c_1c_2c_3)$  be a 3-cycle (in  $A_n$ ). Let  $\delta \in S_n$  be such that  $\delta(a_i) = c_i$ ,  $i = 1, 2, 3$ , and  $\delta\sigma\delta^{-1} = \gamma$ . If  $\delta \in A_n$ , we are done. Suppose  $\delta$  is an odd permutation. Since  $n \geq 5$ , there are two elements  $x_1, x_2 \in [n] \setminus \{a_1, a_2, a_3\}$ . Let  $\delta(x_1) = y_1$  and  $\delta(x_2) = y_2$ . Clearly,  $y_1, y_2 \notin \{c_1, c_2, c_3\}$ . Consider  $\delta' \in S_n$  such that  $\delta'$  coincides with  $\delta$  on all elements of  $[n]$  different from  $x_1, x_2$ ,  $\delta'(x_1) = y_2$  and  $\delta'(x_2) = y_1$ . Then  $\delta' = (y_1, y_2)\delta$  is an even permutation, and  $\delta'\sigma\delta'^{-1} = \gamma$ .  $\square$

**Lemma 2.**  *$N$  contains at least one 3-cycle.*

*Proof.* Since  $N$  contains an even permutation  $\pi \neq e$ , then the representation of  $\pi$  as a product of disjoint cycles must satisfy at least one of the following four conditions. When we say ‘ $\pi$  contains’, we mean ‘the representation of  $\pi$  as the product of disjoint cycles contains’.

- (i)  $\pi$  contains at least one cycle of length at least 4;
- (ii)  $\pi$  contains at least one cycle of length 3 and another cycle of length at least 2;
- (iii)  $\pi$  is a 3-cycle;
- (iv)  $\pi$  contains two disjoint 2-cycles (two disjoint transpositions).

Hence,  $\pi$  can be written in one of these ways, where symbols  $1, 2, \dots, 5$  are chosen just for convenience:

- (i)  $\pi = (1234\dots)\dots$
- (ii)  $\pi = (123)(45\dots)\dots$
- (iii)  $\pi = (123)$ . In this case our lemma is proven.
- (iv)  $\pi = (12)(34)\dots$

Note that for every  $\sigma \in A_n$ , and every  $\pi \in N \trianglelefteq A_n$ , then  $[\pi, \sigma] := (\sigma\pi\sigma^{-1})\pi^{-1} \in N$ .

- In case (i), take  $\sigma = (123)$ . Then  $[\pi, \sigma] = (124)$ .
- In case (ii), take  $\sigma = (124)$ . Then  $[\pi, \sigma] = (12534)$ .
- In case (iv), take  $\sigma = (123)$ . Then  $[\pi, \sigma] = (13)(24)$ .

Therefore case (ii) is reduced to case (i), which, in its turn, is reduced to case (iii). Hence, in cases (i) and (ii), our lemma is also proven.

What is left is to consider case (iv). As  $\alpha = [\pi, \sigma] = (12534)$  is even, and  $(13)(24) \in N$ ,

$$\alpha^{-1} (13)(24) \alpha = (13)(45) \in N,$$

and so  $(13)(24) \cdot (13)(45) = (24)(45) = (245) \in N$ . This ends the proof of Lemma 2.  $\square$

Lemmas 1 and 2 imply Theorem 1.  $\square$

This exposition is my modification of the proof in

M.I. Kargapolov, J.I. Merzljakov, *Fundamentals of the theory of groups*, Springer, 1979.