SIMPLICITY OF ALTERNATING GROUPS A_n, $n \geq 5$.

We are going to prove the following important result, due to Galois:

Theorem 1. *The alternating groups A_n are simple for $n \geq 5$.*

There are several different proofs of this theorem. The one we are going to present is perhaps the most straighforward but it requires some explicit computations with permutations. For different proofs consult [**?**] and [**?**].

Proof: We start with the following observations about the alternating groups (see Problem 4 from homework 3):

(1) *A_n is generated by the set of all 3-cyclces for $n \geq 3$.*

In fact, A_n consists of elements which are products of an even number of transpositions, so it suffices to show that any product of two transpositions $(a, b)(c, d)$ is a product of 3-cycles. If the transpositions (a, b) and (c, d) are disjoint then

$$(a, b)(c, d) = (a, b)(a, c)(a, c)(c, d) = (a, c, b)(c, d, a).$$

If $\{a, b\}$ and $\{c, d\}$ have exactly one element in common, we may assume that $b = d$ so

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

Finally, if $\{a, b\} = \{c, d\}$ then $(a, b)(c, d) = 1$. This shows that each element of A_n is a product of 3-cycles.

Here is our second observation.

(2) *For $n \geq 5$, any two 3-cycles in A_n are conjugate.*

In order to justify this, let (a, b, c) be a 3-cycle in A_n. There is a permutation $\tau \in S_n$ such that $\tau(1) = a$, $\tau(2) = b$, $\tau(3) = c$. It follows that $\tau(1, 2, 3)\tau^{-1} = (a, b, c)$. Let $\sigma = \tau(4, 5)$. Since $(1, 2, 3)$ and $(4, 5)$ commute, we see that $\sigma(1, 2, 3)\sigma^{-1} = (a, b, c)$.

But either τ or σ is even, so $(1,2,3)$ and (a,b,c) are conjugate in A_n. Thus any 3-cycle in A_n is conjugate to $(1,2,3)$. Since being conjugate is an equivalence relation, any two 3-cycles are conjugate in A_n.

We are ready to prove Theorem 1. Suppose that $H \neq \{1\}$ is a normal subgroup of A_n, $n \geq 5$. We will show that H contains a 3-cycle. By (2) this implies that H contains all 3-cycles, so $H = A_n$ by (1).

Consider a non-trivial elelemnt σ in H and let $k > 1$ be the order of σ. Take a prime divisor p of k. Then $\tau = \sigma^{k/p}$ has order p. A permutation of prime order p is a product of disjoint p-cycles, so $\tau = \pi_1 ... \pi_s$ is a product of disjoint $p-$cycles $\pi_1, \ldots, \pi_s$.

We consider three cases:

case 1: $p > 3$

Let $\pi_1 = (a_1, ..., a_p)$. Since H is normal, $\tau_1 = (a_1,a_2,a_3)\tau(a_1,a_2,a_3)^{-1} \in H$. Note that the 3-cycle (a_1,a_2,a_3) commutes with π_i for $i > 1$ so

$$\tau_1 = (a_1,a_2,a_3)\tau(a_1,a_2,a_3)^{-1} = (a_1,a_2,a_3)\pi_1(a_1,a_2,a_3)^{-1}\pi_2 ... \pi_s.$$

Since H is a subgroup, $\tau\tau_1^{-1} \in H$, i.e.

$$\tau\tau_1^{-1} = \pi_1(a_1,a_2,a_3)\pi_1^{-1}(a_1,a_2,a_3)^{-1} = (a_2,a_3,a_4)(a_1,a_3,a_2) = (a_1,a_4,a_2) \in H.$$

We see that H contains a $3-$cycle, i.e. $H = A_n$ in this case.

case 2: $p = 3$

If $s = 1$ then τ is a $3-$cycle in H so $H = A_n$. Otherwise, $s \geq 2$ and $\pi_1 = (a_1,a_2,a_3)$, $\pi_2 = (a_4,a_5,a_6)$. Consider $\tau_1 = (a_1,a_2,a_4)\tau(a_1,a_2,a_4)^{-1}$. Since H is normal, $\tau_1 \in H$. Note that (a_1,a_2,a_4) commutes with π_i for $i \geq 3$. Thus

$$\begin{aligned}
\tau_1 &= (a_1,a_2,a_4)\tau(a_1,a_2,a_4)^{-1} \\
&= [(a_1,a_2,a_4)\pi_1(a_1,a_2,a_4)^{-1}][(a_1,a_2,a_4)\pi_2(a_1,a_2,a_4)^{-1}]\pi_3 ... \pi_s \\
&= (a_2,a_4,a_3)(a_1,a_5,a_6)\pi_3 ... \pi_s.
\end{aligned}$$

Therefore

$$\tau\tau_1^{-1} = (a_1, a_2, a_3)(a_4, a_5, a_6)(a_1, a_6, a_5)(a_2, a_3, a_4) = (a_1, a_4, a_3, a_5, a_2).$$

Since $\tau\tau_1^{-1} \in H$, we see that H contains a $5-$cycle, i.e. an element of order 5. This reduces case 2 to case 1, so $H = A_n$.

case 3: $p = 2$

Since τ is even, s is even and we can write $\pi_1 = (a_1, a_2)$ and $\pi_2 = (a_3, a_4)$. Consider $\tau_1 = (a_1, a_2, a_3)\tau(a_1, a_2, a_3)^{-1} = (a_2, a_3)(a_1, a_4)\pi_3...\pi_s$. We have

$$\rho = \tau\tau_1^{-1} = (a_1, a_2)(a_3, a_4)(a_2, a_3)(a_1, a_4) = (a_1, a_3)(a_2, a_4) \in H.$$

Let a_5 be any number from $\{1, 2, \ldots, n\}$ different from a_1, a_2, a_3, a_4 (it exists, since $n \geq 5$). Then

$$\rho_1 = (a_1, a_3, a_5)\rho(a_1, a_3, a_5)^{-1} = (a_3, a_5)(a_2, a_4) \in H,$$

so H contains the permutation $\rho\rho_1^{-1}$ and

$$\rho\rho_1^{-1} = (a_1, a_3)(a_3, a_5) = (a_3, a_5, a_1).$$

We see that H contains a $3-$cycle, so $H = A_n$.

We proved that in all cases $H = A_5$, so indeed A_n is simple. $\square$

Corollary 1. *If $n \geq 5$ then $\{1\}$, A_n and S_n are the only normal subgroups of S_n.*

Proof: Let $H \triangleleft S_n$, $H \neq \{1\}$. Since $(H \cap A_n) \triangleleft A_n$ and A_n is simple, we see that either $H \cap A_n = A_n$ or $H \cap A_n = \{1\}$. In the first case $A_n < H$, so either $H = A_n$ or $H = S_n$. In the second case, the quotient homomorphism $S_n \longrightarrow S_n/A_n$ is injective on H, so $|H| = 2$. Thus $H = \{1, \tau\}$ for some permutation $\tau \neq 1$. Since H is normal, we must have $\sigma\tau\sigma^{-1} = \tau$ for every $\sigma \in S_n$. We will show that this is not possible. There are $i, j \in \{1, ..., n\}$ such that $\tau(i) = j \neq i$. Take k different from i and j. There is $\sigma \in S_n$ such that $\sigma(i) = i$ and $\sigma(j) = k$. We have $\sigma\tau\sigma^{-1}(i) = k$, so $\sigma\tau\sigma^{-1} \neq \tau$. It follows that $H \cap A_n = \{1\}$ is not possible, so the result follows. $\square$

Exercise. Describe all subgroups and normal subgroups of S_3 and S_4.

References

[1] D. S. Dummit, R. M. Foote, **Abstract Algebra**, second edition, John Wiley & Sons, Inc., 1999.

[2] I. N. Herstein, **Abstract Algebra**, third edition, Prentice-Hall, 1996.