MORE ABOUT SYMMETRIC GROUPS

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 [1] and [2].

Proof: We start with the following observations about the alternating groups:

(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 is generated by the set of elements of the form $(a, b)(c, d)$. If (a, b) and (c, d) are disjoint then we can write

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

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.

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

Let (a, b, c) be a $3-$cycle in A_n. There is $\tau \in S_n$ such that $\tau(1) = a$, $\tau(b) = 2$, $\tau(c) = 3$. 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 $(1, 2, 3)$, so all $3-$cycles are conjugate in A_n.

Suppose now 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).

Let $1 \neq \sigma \in H$ and set k for the order of σ. There is a prime number $p|k$ and then $\tau = \sigma^{k/p}$ has order p. Consequently, $\tau = \pi_1 ... \pi_s$ is a product of disjoint $p-$cycles. We consider three cases:

case 1: $p > 3$

Let $\pi_1 = (a_1, ..., a_p)$. Thus

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

It follows that

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

Hence 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

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

Thus

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

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

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

Now

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

so

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

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

We see that in all cases $H = A_5$, so indeed A_n is simple. □

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

Proof: Let $H \lhd S_n$, $H \neq \{1\}$. Since $(H \cap A_n) \lhd A_n$ 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 natural projection $S_n \longrightarrow S_n/A_n$ is injective on H, so $|H| = 2$. If $1 \neq \tau \in H$ then $\tau(i) = j \neq i$ for some $i, j \in \{1, ..., n\}$.There is $\sigma \in S_n$ such that $\sigma(i) = i$ and $\sigma(j) = k \neq j$. We have $\sigma\tau\sigma^{-1} = \tau_1 \in H$ and $\tau_1(i) = k$. It follows that $1, \tau, \tau_1$ are three distinct elements in H, a contradiction. Thus $H \cap A_n = \{1\}$ is not possible, so the result follows. □

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.