The simplicity of the alternating groups

September 16, 2010

Theorem 0.1 *If $n \geq 5$, the alternating group A_n is simple.*

Proof: We proved that A_5 is simple by computing its conjugacy classes. We continue by induction.

Lemma 0.2 *Let A be a set with n elements. Then the action of S_A on A is m-fold transtive for all $m \leq n$, and the action of A_A on A is m-fold transitive for all $m \leq n-2$.*

Proof: Suppose that $1 \leq m \leq n$ and $(a_1, \ldots, a_m)$ and $(b_1, \ldots, b_m)$ are injective sequences in A. There is evidently an element σ of S_A taking each a_i to b_i. This shows that the action of S_A is m-fold transitive. Now if $m \leq n-2$ and the σ chosen above is not in A_A, there at least two elements, say c_1 and c_2, in $\{1, \ldots, n\}$ which are not equal to any of the b_i's. Then the $\sigma' := (c_1 c_2)\sigma$ is in A_A and has the same effect on the a_i's as does σ. □

It follows from this that if $n \geq 3$, the standard action of A_n is transitive, and if $n \geq 4$, it is doubly transtive, hence primitive.

Corollary 0.3 *Let G be a group of order n and let $G^* := G \setminus \{e\}$. The action of $Aut(G)$ leaves G^* invariant and thus there is an injective group homomorpism $Aut(G) \to S_{G^*}$. If $n \geq 5$, the image of this map cannot contain all of A_{G^*}.*

(Remark: if $G = \mu_2 \times \mu_2$, its autmorphism group is in fact all of S_{G^*}).

Proof: Say $n \geq 5$. Then A_{G^*} acts 3-fold transitively on G^*. Choose $g_1 \in G^*$ and then g_2 such that $g_2 \neq g_1, g_1^{-1}$. Note that there is at least one more element g_3 in G^* with $g_3 \neq g_1, g_2$ and $\neq g_1 g_2$. Then no automorphism of G can map $(g_1, g_2, g_1 g_2)$ to (g_1, g_2, g_3). □

Now we prove that if $n \geq 6$, A_n is simple. We assume that A_{n-1} is simple. Note that A_{n-1} is the stabilizer of n via the standard action of A_n. Since the action of A_n is doubly transitive, it is primitive, so there is no subgroup strictly between A_{n-1} and A_n. Suppose that N were a nontrivial proper normal subgroup of A_n. Since A_{n-1} is maximal maximal, it cannot be the case that $A_{n-1} \subseteq N$ (equality is impossible because A_{n-1} is not normal). Then $N \cap A_{n-1}$ is a proper normal subgroup of A_{n-1}. Since A_{n-1} is simple, $N \cap A_{n-1} = \{e\}$. Since NA_{n-1} is a subgroup of A_n containing A_{n-1} and hence is all of A_n. Since $N \cap A_{n-1} = \{e\}$, N has order n, and A_n is the semidirect product of N and A_{n-1} with respect to some homomorphism $\alpha\colon A_{n-1} \to Aut(N)$. This homomorphism can't be tivial, since A_{n-1} is not normal. By the simplicty of A_{n-1}, the kernel of α is trivial. But then the imageof $Aut(N)$ in S_{N^*} would contain a subgroup of index 2, necessarily the alternating group, which we saw is impossible when $n \geq 5$. □