Mathematics 4340
Simplicity of the alternating groups
Ken Brown, Cornell University, February 2009

Recall that we gave an ad hoc proof in class that A_5 is simple. This proof is also in the book (p. 128), and there is a second ad hoc proof on p. 145. The book goes on in Section 4.6 to prove the simplicity of A_n for $n > 5$. I'll give here a different proof, based on fairly general principles that are used in a lot of simplicity proofs.

The key idea is to play with the *commutator* $[g, h] := ghg^{-1}h^{-1}$. Notice that we can think of this either as g times a conjugate of g^{-1} or as a conjugate of h times h^{-1}. We will exploit these two ways of thinking about the commutator in our proof. [You've actually seen this idea already in Exercise 3.1.42, where you proved that if two normal subgroups have trivial intersection, then the elements of one commute with those of the other.]

The first step is to find a set of generators for A_n having small support (i.e., moving few points): I claim that A_n is generated by 3-cycles; moreover, any two 3-cycles are conjugate if $n \geq 5$. For the first assertion, it suffices to observe that a product of two distinct transpositions is either a 3-cycle or a product of two 3-cycles. The typical cases are $(1\ 2)(2\ 3) = (1\ 2\ 3)$ and $(1\ 2)(3\ 4) = (1\ 4\ 3)(1\ 2\ 3)$. For the second assertion, recall first that any two 3-cycles σ, τ are conjugate in S_n, say $g\sigma g^{-1} = \tau$. If g happens to be an odd permutation, replace it by gh, where h is a transposition that centralizes σ. [This exists because $n \geq 5$.]

Now suppose $1 \neq H \trianglelefteq A_n$ ($n \geq 5$). In view of the claim that we've just proved, the simplicity of A_n will follow if we can show that H contains a 3-cycle. So our strategy will be to try to find an element $h \in H$ with the simplest possible cycle structure, until we eventually find a 3-cycle in H.

Start with any nontrivial $h \in H$, say $h(1) = 2$. Let g be any 3-cycle that doesn't involve 2, e.g., $g = (1\ 3\ 4)$, and consider the commutator $[g, h]$. Thinking of the commutator as kh^{-1}, where k is a conjugate of h, we see that it is in H. But we can also view $[g, h]$ as $g(hg^{-1}h^{-1})$, so it is a product of two 3-cycles, $(1\ 3\ 4)(2\ h(4)\ h(3))$. The presence of 2 in only one spot shows that $[g, h] \neq 1$. Replacing h by this commutator, then, we now have a nontrivial $h \in H$ that is a product of two 3-cycles! Let's try to simplify it further.

Suppose first that the two 3-cycles are disjoint, so that h has a cycle decomposition of the type $h = (1\ 2\ 3)(4\ 5\ 6)$. All permutations of this type are conjugate in A_n, since $(1\ 2\ 3)(4\ 5\ 6)$ is centralized by the odd permutation $(1\ 4)(2\ 5)(3\ 6)$. So H contains all of them. In particular, H contains $k := (1\ 2\ 3)(4\ 5\ 6)^{-1}$, and the product kh is a 3-cycle in H, as desired.

Suppose now that the two 3-cycles are not disjoint. Then h moves at most 5 points, so h is contained in an isomorphic copy of A_5 inside A_n. Thus $H' := H \cap A_5$ is a nontrivial normal subgroup of A_5 and hence is all of A_5, since we already know that the latter is simple. In particular, H' contains a 3-cycle, and the proof is complete.

What made this proof work, aside from some ad hoc arguments once we got down to A_5? I see two general principles: (a) If $H \trianglelefteq G$, then H is closed under the operation of forming commutators with arbitrary elements of G. (b) If g has "small support", then $[g, h]$ is often simpler than h [because it is the product of g and something that resembles g].