Proof that the group A_n is simple for all $n \geq 5$

Let n be an integer ≥ 5.

To show that the alternating group A_n is simple, we must show that any normal subgroup of A_n which contains a nonidentity element x must be all of A_n. What this comes down to showing is that starting with any such x, we can, by using the group operations and the operations of conjugating by various elements of A_n, eventually come up with every other element $y \in A_n$. Now to get from *any* nonidentity element x to *any* other element y is a formidable task. To make it more manageable, we shall go via an easy-to-handle intermediate class of group elements. The even permutations that move the *smallest* number of elements are the cycles of length 3; and the main steps of our proof will in fact be:

Step I. If a normal subgroup N of A_n contains a nonidentity element x, then it contains a cycle (a_1, a_2, a_3) of length 3.

Step II. If a normal subgroup N of A_n contains a cycle of length 3, then it contains every cycle of length 3.

Step III. If a subgroup N of A_n contains every cycle of length 3, then it is all of A_n.

Of these, Step I is the most work. The idea is as follows. Let us say that an element $i \in \{1, \ldots, n\}$ is ''moved by σ'' if $\sigma(i) \neq i$; in the contrary case we will say that i is ''fixed by σ''; and let us think of a permutation as ''small'' if it moves few elements of $\{1, \ldots, n\}$. If x is any element of N and σ a ''small'' even permutation, then the conjugate $\sigma x \sigma^{-1}$, which by normality of N also lies in N, will differ only ''slightly'' from x; i.e., will agree with x except on a small number of elements. Hence if we ''divide'' the former element by the latter, the resulting permutation, $(\sigma x \sigma^{-1}) x^{-1}$, will be relatively ''small''. By applying this principle with a little ingenuity, we will be able to get from an arbitrarily ''large'' permutation down to a cycle of length 3.

Let us begin with a lemma making explicit the computational trick sketched above.

Lemma 1. *Let $x, \sigma \in A_n$. Then every element $i \in \{1, \ldots, n\}$ that is moved by $\sigma x \sigma^{-1} x^{-1}$ is either an element moved by σ, or the image under x of an element moved by σ.*

Proof. Suppose $i \in \{1, \ldots, n\}$ is neither an element moved by σ nor the image under x of such an element. The latter condition implies that the element whose image under x is i, namely $x^{-1}(i)$, is not moved by σ, hence is not moved by σ^{-1} either. Hence we get $\sigma x \sigma^{-1} x^{-1}(i) = \sigma(x(\sigma^{-1}(x^{-1}(i)))) = \sigma(x(x^{-1}(i))) = \sigma(i) = i$ as required. (The second step, i.e., the second ''='', uses the fact that $x^{-1}(i)$ is not moved by σ, the third step uses the identity $x x^{-1} = \iota$, and the last step, the assumption that i is not moved by σ.) $\square$

Now let N be any nontrivial normal subgroup of A_n. We shall apply the above lemma in each of a series of cases, to show that in every case, N contains a cycle of length 3. We shall also use repeatedly the fact that if $x \in N$ and $\sigma \in A_n$, then $\sigma x \sigma^{-1} x^{-1}$ is the product of the two elements $\sigma x \sigma^{-1}$ and x^{-1} of N, and hence also a member of N.

Case A. N contains an element x whose expression as a product of disjoint cycles involves at least one cycle of length greater than 3.

Let such a cycle be $(a_1, a_2, a_3, a_4, \ldots, a_r)$. (Here r may equal 4, so the '' $\ldots, a_r$ '' may be empty; but since $r > 3$, a_1, a_2, a_3, a_4 are distinct.) Thus, $x = (a_1, a_2, a_3, a_4, \ldots, a_r) P$, where P is either the identity, or a product of cycles that do not move any of $a_1, \ldots, a_r$. Let $\sigma = (a_1, a_2, a_3)$. The elements of $\{1, \ldots, n\}$ that are moved by σ are a_1, a_2, a_3, and the images under x of those elements are a_2, a_3, a_4. Hence by Lemma 1, the permutation $\sigma x \sigma^{-1} x^{-1}$ cannot move any elements but a_1, a_2, a_3, a_4. Therefore we can describe $\sigma x \sigma^{-1} x^{-1}$ by determining what it does on those four elements. Go through this calculation. You will find that $\sigma x \sigma^{-1} x^{-1} = (a_1,\ a_2,\ a_4)$. Hence in this case N indeed contains a cycle of length 3, as claimed.

Now if a nonidentity element $x \in N$, when expressed as a product of disjoint cycles, does *not* involve a cycle of length greater than 3, then it must be a product of disjoint cycles each of length 2 or length 3. Also note that if an element x is written as a product of disjoint cycles $\sigma_1 \dots \sigma_r$, then $\sigma_1, \dots, \sigma_r$ commute with each other; hence for any integer d, we have $x^d = \sigma_1^d \dots \sigma_r^d$. In particular, if the x we are interested in here involves *both* cycles of length 2 and cycles of length 3, then x^2 involves only cycles of length 3 (since the square of a cycle of length 2 is the identity, while the square of a cycle of length 3 is another cycle of length 3); and similarly, x^3 involves only cycles of length 2. Thus by either squaring or cubing such an x, we can see that N contains an element which is either a product of one or more disjoint cycles of length 2, or of one or more disjoint cycles of length 3. We now consider those cases:

Case B. N contains an element x which is a product of one or more disjoint cycles of length 3. If x is a single cycle of length 3, we have what we want. In the contrary case, let us write it as $(a_1, a_2, a_3)\,(a_4, a_5, a_6)\,P$, where P is again either the identity or a product of cycles that do not move any of $a_1, \dots, a_6$. In this case, let us take $\sigma = (a_2,\ a_3,\ a_4)$. Using Lemma 1, we find that $\sigma x \sigma^{-1} x^{-1}$ can only move some subset of $\{a_1, \dots, a_5\}$. Calculating, we find that $\sigma x \sigma^{-1} x^{-1} = (a_1, a_4, a_2, a_3, a_5)$, a cycle of length 5. Applying the result of Case A, we conclude that N also contains a cycle of length 3.

Case C. N contains an element x which is a product of one or more disjoint cycles of length 2. In this case there must be at least two such cycles, since a single cycle of length 2 is an odd permutation, while N was assumed a subgroup of the group A_n of even permutations. Hence let us write $x = (a_1, a_2)\,(a_3, a_4)\,P$, with P as before. Taking $\sigma = (a_1,\ a_2,\ a_3)$, we find that $\sigma x \sigma^{-1} x^{-1} = (a_1, a_3)(a_2, a_4)$.

This is still a product of cycles of length 2, so have we accomplished anything? Yes, we have gotten rid of P, and thus have a member of N which moves only 4 elements of $\{1, \dots, n\}$. Since $n \geq 5$, this means that at least one element is fixed by this permutation. And this puts us in our final case:

Case D. N contains an element x such that the expression for x as a product of disjoint cycles involves a cycle (a_1, a_2) of length 2*, and such that x fixes at least one element a_3*. In this situation, let us write $x = (a_1, a_2)\,P$ where P moves none of a_1, a_2, a_3, and let $\sigma = (a_1, a_2, a_3)$. By Lemma 1, $\sigma x \sigma^{-1} x^{-1}$ can move only some subset of $\{a_1, a_2, a_3\}$. Computing its action on this set, you will find that it equals (a_1, a_3, a_2), a cycle of length 3. This completes our proof that in every case, N contains such an element.

For Step II of our proof, we must show that if N contains a cycle (a_1, a_2, a_3) of length 3, it contains every cycle (b_1, b_2, b_3) of that length. To do this, we will need an explicit formula for the result of conjugating a cycle of length 3 by any other permutation σ. I claim that such a formula is

$$\sigma\,(a_1, a_2, a_3)\,\sigma^{-1} \;=\; (\sigma(a_1),\ \sigma(a_2),\ \sigma(a_3)).$$

Indeed, it is easy to see that the two sides agree on the three elements $\sigma(a_1)$, $\sigma(a_2)$ and $\sigma(a_3)$. If i is not one of these elements, then $\sigma^{-1}(i)$ is not one of a_1, a_2 or a_3, hence it is not moved by the cycle

(a_1, a_2, a_3), so $\sigma\,(a_1, a_2, a_3)\,\sigma^{-1}(i) = \sigma\sigma^{-1}(i) = i$; so the left-hand side of the above display agrees with the right-hand side on such elements i as well.

Hence if our subgroup N contains a cycle (a_1, a_2, a_3) and we want to show it to contain some other cycle of length 3, (b_1, b_2, b_3), the obvious thing to do is find a permutation σ such that $\sigma(a_1) = b_1$, $\sigma(a_2) = b_2$, $\sigma(a_3) = b_3$; which we can do, roughly speaking, by writing $\sigma = \begin{pmatrix} \dots\ a_1 \dots\ a_2 \dots\ a_3 \dots \\ b_1 \quad b_2 \quad b_3 \end{pmatrix}$ and filling in the remaining entries of the bottom row in any way such that each integer from 1 to n gets used exactly once. (I say ''roughly speaking'' because the way I have written this permutation assumes $a_1 < a_2 < a_3$. When that is not so, the columns shown will appear in a different order.)

This will indeed give us a permutation σ such that $\sigma(a_1, a_2, a_3)\,\sigma^{-1} = (b_1, b_2, b_3)$; and if this σ is even, i.e., is a member of A_n, that will show that the normal subgroup N of A_n, in addition to (a_1, a_2, a_3), also contains (b_1, b_2, b_3). But what if σ is odd? There are various ways one can ''cure'' this; the one we will use is to let $\sigma' = (b_2, b_3)\sigma$. Since (b_2, b_3) is, like σ, odd, σ' will be even. It will again send the three elements a_1, a_2, a_3 to b_1, b_2, b_3, but in a different order; and we see that $\sigma'(a_1, a_2, a_3)\,\sigma'^{-1} = (b_1, b_3, b_2)$. Now the *square* of this cycle is the desired cycle (b_1, b_2, b_3); so again, if N contains (a_1, a_2, a_3), it also contains (b_1, b_2, b_3), completing Step II.

For Step III, we must prove that the cycles of length 3 together generate A_n. A key fact will be

Lemma 2. *If x is a permutation which moves at least three elements, then there exists a cycle σ of length 3 such that $\sigma^{-1}x$ moves fewer elements than x does.*

Proof. Let a_1 be an element moved by x. If we write $a_2 = x(a_1)$, this is a second element moved by x. Since there are at least three elements moved by x, we can choose a third such element, a_3. Letting $\sigma = (a_1, a_2, a_3)$, we observe that $\sigma^{-1}x$ does not move any elements that are not moved by x (since neither x nor σ^{-1} does); hence if we can prove that $\sigma^{-1}x$ fixes some element that is moved by x, we will have the desired conclusion. And indeed, it is immediate from the way we defined σ that $\sigma^{-1}x$ fixes a_1. $\square$

Since the only permutations that move fewer than three elements are the identity and the transpositions, we see that every nonidentity element of A_n moves at least three elements. Hence if x is a nonidentiy element of A_n, we can use the above lemma to find a cycle σ_1 of length 3 such that $\sigma_1^{-1}x$ moves fewer elements than x. If $\sigma_1^{-1}x$ is not the identity, we can similarly use the lemma to find a cycle σ_2 of length 3 such that $\sigma_2^{-1}\sigma_1^{-1}x$ moves fewer elements than $\sigma_1^{-1}x$, and so forth. This process must eventually stop, so we must eventually get an expression for the identity permutation as

$$\sigma_r^{-1} \dots \sigma_1^{-1} x$$

where $\sigma_1, \dots, \sigma_r$ are cycles of length 3. This condition can be written $(\sigma_1 \dots \sigma_r)^{-1}x = \iota$, equivalently, $x = \sigma_1 \dots \sigma_r$, showing that the general element x of A_n is indeed a product of cycles of length 3.

In summary, we have shown that for $n \geq 5$, any normal subgroup N of A_n which contains a nonidentity element contains a cycle of length 3, from this that N contains *all* cycles of length 3, and from this that N contains all elements of A_n. Thus A_n has no proper nontrivial normal subgroup; i.e., it is simple.