A_n is simple, $n \geq 5$

See Herstein, Section 6.1

To prove that A_n is simple for $n \geq 5$, we need a few lemmas ("baby theorems").

Lemma
If $n \geq 3$, then the only permutation in S_n that commutes with every transposition is the identity permutation e.

Proof:
Suppose $\sigma \in S_n$ commutes with every transposition, but $\sigma \neq e$. Then there is some $i \in \{1, \ldots, n\}$ s.t. $\sigma(i) = j \neq i$. Since $n \geq 3$, there is a third number $k \in \{1, \ldots, n\}$ different from both i & j. Let $\tau = (i\ k)$. Then

$$\sigma(k) = \sigma\tau(i) = \tau\sigma(i) = \tau(j) = j.$$

But we also have $\sigma(i) = j$, so since σ is a bijection, this implies $i = k$, which is a contradiction. ▨

Corollary
For $n \geq 3$ the center of S_n is $Z(S_n) = \{e\}$.

Lemma
If τ is a transposition, then $\sigma\tau\sigma^{-1}$ is also a transposition for every $\sigma \in S_n$.

Proof:
Suppose $\tau = (i\ j)$ and $\sigma \in S_n$. We'll show that $\sigma\tau\sigma^{-1} = (\sigma(i)\ \sigma(j))$. First,

$$(\sigma\tau\sigma^{-1})(\sigma(i)) = \sigma\tau(i) = \sigma(j)$$

$$(\sigma\tau\sigma^{-1})(\sigma(j)) = \sigma\tau(j) = \sigma(i).$$

Thus $\sigma\tau\sigma^{-1}$ does interchange $\sigma(i)$ & $\sigma(j)$.

Suppose $k \neq \sigma(i), \sigma(j)$. Then $\sigma^{-1}(k) \neq i, j$ (why?), so τ fixes $\sigma^{-1}(k)$, and therefore

$$(\sigma\tau\sigma^{-1})(k) = \sigma\tau(\sigma^{-1}(k)) = \sigma\sigma^{-1}(k) = k.$$

Thus $\sigma\tau\sigma^{-1}$ fixes all k other than $\sigma(i), \sigma(j)$, so $\sigma\tau\sigma^{-1}$ is the transposition $(\sigma(i)\ \sigma(j))$. ∎

Lemma
If a normal subgroup N of S_n contains a 3-cycle, then it contains every 3-cycle.

Proof:
Suppose $N \triangleleft S_n$ and $(a\ b\ c) \in N$. Choose any 3-cycle $(j\ k\ l)$.

Case 1: a, b, c are all different than j, k, l.

In this case, since a transposition is its own inverse, we have $\tau\,(a\ b\ c)\,\tau \in N$ for every transposition τ. Repeating this, we see that

$$(c\ l)(b\ k)(a\ j)(a\ b\ c)(a\ j)(b\ k)(c\ l) = (j\ k\ l)$$

belongs to N.

Case 2: Some of a, b, c coincide with some j, k, l.

Exercise: Show we can still conclude $(j\ k\ l) \in N$. ∎

Lemma

If a normal subgroup N of S_n contains a 3-cycle, then $N \supseteq A_n$. Consequently, either $N = A_n$ or $N = S_n$.

Proof:

Suppose $N \triangleleft S_n$ & N contains a 3-cycle. Then by the preceding lemma, N contains every 3-cycle.

We must show that N contains every even permutation. Every even permutation is a product of an even number of transpositions. So, we just have to show that N contains every product of two transpositions, because it then contains all products of these.

Case 1: $(i\ j)(k\ l)$ with i, j, k, l all distinct.

$$(i\ j)(k\ l) = (i\ l\ j)(i\ l\ k) \in N$$

since N contains every 3-cycle.

Case 2: $(i\ j)(i\ l)$ with i, j, l distinct.

$$(i\ j)(i\ l) = (i\ l\ j) \in N.$$

Case 3: $(i\ j)(i\ j)$

This is e, which belongs to N.

Thus, N contains all even permutations, hence $N \supseteq A_n$. But $|A_n| = \frac{1}{2}|S_n|$, so the only possibilities are $N = A_n$ or $N = S_n$ (why?). ∎

Also, the fact that $\tau\sigma \neq \sigma\tau$ implies $\tau\alpha \neq e$ (Why?). Hence τ, α are different transpositions. If we write $\tau = (i\ j)$ and $\alpha = (k\ l)$ then τ & α can have at most one letter in common.

Case 1: τ, α have one letter in common.

In this case we can write $\tau = (i\ j)$ and $\alpha = (i\ l)$, so $\tau\alpha = (i\ j)(i\ l) = (i\ l\ j)$ is a 3-cycle that belongs to N (note that we must have $j \neq l$).

Case 2: τ, α have no letters in common.

In this case $\tau = (i\ j)$ and $\alpha = (k\ l)$ with i, j, k, l all distinct. Since $n \geq 5$, there is a fifth $m \in \{1, \ldots, n\}$ different from i, j, k, l.

We can't quite show yet that A_n is simple, but we can show that it is the only nontrivial normal subgroup of S_n when $n \geq 5$.

Theorem
If $n \geq 5$ then the only normal subgroups of S_n are $\{e\}$, A_n, & S_n.

Proof:
Suppose that N is a normal subgroup of S_n other than $\{e\}$ or S_n. Then $\exists\, \sigma \in N$ with $\sigma \neq e$. By a previous lemma, σ cannot commute with every transposition, so $\exists$ some transposition τ such that $\sigma\tau \neq \tau\sigma$.

By an earlier lemma, $\alpha = \sigma\tau\sigma^{-1}$ is also a transposition. Also, N is normal, so $\tau\sigma\tau = \tau\sigma\tau^{-1} \in N$. Since $\sigma \in N$, we therefore have

$$\tau\alpha = \tau\sigma\tau\sigma^{-1} = (\tau\sigma\tau)(\sigma^{-1}) \in N.$$

Set $\beta = (i\ m)$. Then since $\tau\alpha \in N$ and N is normal,

$$\beta\tau\alpha\beta^{-1} = (i\,m)(i\,j)(k\,\ell)(i\,m) = (j\,m)(k\,\ell)$$

belongs to N. Hence the product of this with $\tau\alpha$ also belongs to N, and this product is

$$(i\,j)(k\,\ell)(j\,m)(k\,\ell) = (i\,j\,m).$$

Thus N contains a 3-cycle.

Thus, in any case, we have shown that N contains a 3-cycle. But then a previous lemma implies that either $N = A_n$ or $N = S_n$. Hence the only normal subgroups are $\{e\}$, A_n, & S_n when $n \geq 5$. ∎

Exercise
Show that

$$N = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$$

is a normal subgroup of S_4, [redacted] & $N \neq A_4$.

Now we can work on showing that A_5 is simple. We need the following definition & exercise.

Definition

If H is a subgroup of a group G, then the normalizer of H in G is

$$N_H = \{a \in G : aHa^{-1} = H\}.$$

Note that if H is normal, then $N_H = G$, but if H is not normal, then N_H is a proper subset of G. N_H will always include at least H (why?), and the larger N_H is the "closer to normal" that H is, in some sense.

Exercise

Let H be a subgroup of G, & let N_H be its normalizer. Prove that:

a. N_H is a subgroup of G;

b. $H \triangleleft N_H$ (although H need not be normal in G).

Now we will show that A_5 is simple. Recall that we have already shown that A_5 is the only nontrivial normal subgroup of S_5.

Exercise

Why can't we use the following argument?

"Suppose that N is a nontrivial normal subgroup of A_5. Then since $N \triangleleft A_5$ & $A_5 \triangleleft S_5$, we have $N \triangleleft S_5$. Therefore N is a nontrivial normal subgroup of S_5 and $N \neq A_5$, which contradicts the fact that A_5 is the only nontrivial normal subgroup of S_5."

Show that this argument is flawed. Find an example that shows that the relation "A is a normal subgroup of B" is not transitive, i.e., find a counterexample to:

$$K \triangleleft H \;\&\; H \triangleleft G \implies K \triangleleft G.$$

Theorem A_5 is simple.

Proof:

Note that $|A_5| = \frac{1}{2}|S_5| = \frac{1}{2}5! = 60$.

Suppose that A_5 was not simple. Then it would have one or more nontrivial normal subgroups, say $N_1, \ldots, N_k$. The orders $|N_1|, \ldots, |N_k|$ are integers between 2 & 30 (why?). Out of all these orders there's a smallest one (not necessarily uniquely – there may be several N_j that all have the same smallest order). Choose any one of these with smallest order & call it N.

Let $K = \{\sigma \in S_5 : \sigma N \sigma^{-1} = N\}$ be the normalizer of N in S_5. Then by an exercise, K is a subgroup of S_5, & $N \trianglelefteq K$. Now, we know that $N \trianglelefteq A_5$, which means that $\sigma N \sigma^{-1} = N \quad \forall \sigma \in A_5$. Hence $A_5 \subseteq K$.

Thus we have $A_5 \subseteq K \subseteq S_5$. Since K is a subgroup, this implies $|A_5| \mid |K|$ & $|K| \mid |S_5|$. But $|A_5| = \frac{1}{2}|S_5|$. There are only two possibilities: $K = A_5$ or $K = S_5$ (why?). But if $K = S_5$ then $\sigma N \sigma^{-1} = N$ for all $\sigma \in S_5$, which implies $N \triangleleft S_5$, contradicting the fact that A_5 is the only nontrivial normal subgroup of S_5. Therefore we conclude that $K = A_5$, i.e.,

$$\sigma N \sigma^{-1} = N \iff \sigma \in A_5.$$

Consequently, since $\sigma = (1\,2)$ is an odd permutation, it does not belong to A_5, and hence

$$M = (1\,2)\,N\,(1\,2) \neq N.$$

Exercise: Prove the following facts.

a. $M \triangleleft A_5$

Hint: This is a consequence of the fact that $N \triangleleft A_5$.

b. $M \cap N \triangleleft A_5$

c. $MN \triangleleft A_5$.

Now, if $M \cap N \neq \{e\}$, then $M \cap N$ is a nontrivial normal subgroup of A_5 (since $\{e\} \subsetneq M \cap N \subseteq N \subsetneq A_5$). But of all the nontrivial normal subgroups of A_5, N had the smallest possible order. Therefore $M \cap N$ cannot be smaller than N, so $M \cap N = N$.

On the other hand, we also have $\{e\} \subsetneq M \cap N \subseteq M \subsetneq A_5$, so the same reasoning applied to M (which has the same order as N - why?) implies that $M \cap N = M$. But then $M = N$, which is a contradiction.

Hence $M \cap N = \{e\}$. By an earlier exercise, we therefore have $|MN| = |M|\,|N| = |N|^2$. Thus MN is a normal subgroup of A_5 whose order

is a perfect square greater than 1.

We will show that $MN = A_5$. Since $|A_5| = 60$ is not a perfect square, this will be a contradiction.

We already know that $MN \triangleleft A_5$, so

$$\sigma \in A_5 \implies \sigma MN\sigma^{-1} = MN. \qquad (*)$$

Exercise: The fact that M & N are each normal in A_5 implies that $MN = NM$.

Therefore,

$$\begin{aligned}(12)MN(12) &= (12)(12)N(12)N(12) \\ &= N(12)N(12) \\ &= NM \\ &= MN. \qquad (**)\end{aligned}$$

Suppose $\tau \in S_5 \setminus A_5$, i.e., τ is an odd permutation. Then $\sigma = (12)\tau$ is even,

and $\tau = (12)\sigma$, so $\tau^{-1} = \sigma^{-1}(12)$, and hence

$$\begin{aligned} \tau MN\tau^{-1} &= (12)\sigma MN\sigma^{-1}(12) \\ &= (12)MN(12) \qquad \text{from } (*) \\ &= MN \qquad \text{from } (**). \end{aligned}$$

Thus $\tau MN\tau^{-1} = MN$ for <u>every</u> $\tau \in S_5$, so $MN \triangleleft S_5$. But $\{e\} \subsetneq MN \subseteq A_5 \subsetneq S_5$ and A_5 is the <u>only</u> nontrivial normal subgroup of S_5, so $(**)$ implies that $MN = A_5$.

This is a contradiction, because $|MN| = |N|^2$ is a perfect square, but $|A_5| = 60$ is not. Hence no such N can exist, ie., A_5 is simple. ∎

Theorem A_6 is not simple.

Proof:

Repeat the proof given for A_5. It carries over completely, and the only change needed being the fact that $|A_6| = \frac{1}{2}6! = 360$ is not a perfect square. ∎

Remark

If we just knew that $\frac{1}{2}n!$ is never a perfect square, we could extend this argument to arbitrary n. This is one way to prove that A_n is not simple for any $n \geq 5$.

Another way is to show that every nontrivial normal subgroup of A_n must contain a 3-cycle by reducing to the case of A_6. For a proof using this method, see Theorem 6.1.9 in Herstein.

Classification of Finite Simple Groups

We have seen that $A_5, A_6, A_7, \ldots$ is one (infinite) family of finite simple groups. The classification theorem for finite simple groups says that every finite simple groups belongs to one of several specific infinite families, except for 26 particular groups that do not belong to any of these families. These 26 are called the "sporadic groups."

One of these 26 is called the monster group. It is a finite simple group of order

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

which is $\approx 8 \times 10^{53}$.

Of the 26 sporadic groups, 20 are either subgroups or quotients of subgroups of the monster. The remaining 6 groups are sometimes called the pariah groups.

The smallest nonabelian finite simple group is A_5, of order 60.

The smallest sporadic group has order 7920.