Last time: Every element of S_n can be expressed as product of a unique collection of disjoint cycles. Conjugacy classes in S_n correspond to partitions of n, ie. ways to express n as a sum of positive integers (= lengths of the cycles).

$p(n) = \#$ partitions of n $= \#\{a_1,\dots,a_k \,/\, a_1 \geq \dots \geq a_k,\ \sum a_i = n\}$

Or, let $m_j = \#\{i \,/\, a_i = j\}$ number of times j appears in the partition, then $p(n) = \#\{(m_1,\dots,m_n) \in \mathbb{N}^n \,/\, \sum j m_j = n\}$

There is no closed formula for $p(n)$; it grows faster than any polynomial.

Hardy-Ramanujan 1918: $p(n) \sim \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right)$ (this looks hard; it is).

However there are recursive formulas, and also a nice expression for the generating series $f(t) = \sum_{n=0}^{\infty} p(n) t^n = \prod_{j=1}^{\infty} \frac{1}{1-t^j}$. (So: coeff^t of t^n in this product is $p(n)$!)

This is because $\frac{1}{1-t^j} = 1 + t^j + t^{2j} + \dots$ so coeff^t of t^n in the product is #ways of writing n as sum of multiples of j for $j=1,2,\dots$ ie. $n = m_1 + 2m_2 + 3m_3 + \dots$

---

* What is the size of the conjugacy class in S_n corresponding to a given partition $n = \sum j m_j$ (ie. m_1 fixed elements, m_2 2-cycles, m_3 3-cycles, ...)?

Answer: first need to partition $\{1..n\}$ into m_1 subsets of size 1, m_2 of size 2, etc.:

there are $\frac{n!}{(1!)^{m_1}(2!)^{m_2}\dots}$ ways (S_n acts transitively on the set of such decompositions, with stabilizer subgroup $\prod_j (S_j)^{m_j}$ = permutations which permute only within each subset)

But in fact we don't care about ordering of the various subsets of given size. This divides by $m_j!$ for each j (permute the m_j subsets of size j).

so we get $\frac{n!}{\prod_{j\geq 1}\left((j!)^{m_j}\, m_j!\right)}$ partitions of $\{1..n\}$ into unordered collection of subsets of the correct sizes.

Now, in S_j there are $(j-1)!$ j-cycles $(1 \to \underset{j-1 \text{ choices}}{?} \to \underset{j-2 \text{ choices}}{?} \to \dots)$.

so in total $\prod((j-1)!)^{m_j}$ ways of choosing the cycles acting on each subset.

Hence: $|C| = \frac{n!}{\prod_{j\geq 1}(j^{m_j} \cdot m_j!)}$ (If you like combinatorics: can you check by direct calculation that these do add up to $n! = |S_n|$?)

Let's now return to the alternating group $A_n = \mathrm{Ker}(\mathrm{sgn}: S_n \to \{\pm 1\})$

* Observe: a k-cycle has sign $(-1)^{k-1}$. (since $(i_1 \dots i_k) = (i_1\, i_2)(i_2\, i_3)\dots(i_{k-1}\, i_k)$).
So $\sigma \in A_n$ iff its cycle decomposition has an even number of cycles of even length.

* Prop: If $C \subset S_n$ is a conjugacy class then either $C \cap A_n = \emptyset$, or $C \subset A_n$.
In the latter case, either C is a conjugacy class in A_n, or it splits into 2 conjugacy classes in A_n.
C is a single conjugacy class in A_n iff, given $\sigma \in C$, there exists an odd permutation τ that commutes with σ.

Proof: • all elements of C have same cycle lengths $\Rightarrow$ same sign. So $C \subset A_n$ or $C \cap A_n = \emptyset$.
(or: A_n is a normal subgp. of S_n hence a union of conjugacy classes).
• assume $C_\sigma = \{g\sigma g^{-1} \,/\, g \in S_n\} \subset A_n$, then split S_n into the 2 (right) cosets of A_n, $S_n = A_n \cup A_n \cdot \tau$ for any τ with $\mathrm{sgn}(\tau) = -1$. Then

$$C_\sigma = \{h\sigma h^{-1} \,/\, h \in A_n\} \cup \{h\tau\sigma\tau^{-1}h^{-1} \,/\, h\tau \in A_n\tau\}.$$
$$= (\text{conj. class of } \sigma \text{ in } A_n) \cup (\text{conj. class of } \tau\sigma\tau^{-1} \text{ in } A_n)$$

These 2 conj. classes are either equal or disjoint; they are equal iff σ is in the latter conj. class, ie. $\exists\, g = h\tau$ (odd) st. $g\sigma g^{-1} = \sigma$, ie. $g\sigma = \sigma g$. □

In other terms: $\sigma \in C$, $Z(\sigma) = \{\tau \in S_n \,/\, \tau\sigma\tau^{-1} = \sigma\}$ centralizer,
If $Z(\sigma) \subset A_n$ then conjugates of σ by odd permutations are different from conjugates by even permutations, form two conj. classes in A_n; if $Z(\sigma) \not\subset A_n$ then all conjugates of σ in S_n are conjugates by elements of A_n.

Ex: $n=5$; $A_5 = \underset{1}{\{id\}} \cup \underset{15}{\{(ij)(kl)\}} \cup \underset{20}{\{3\text{-cycles}\}} \cup \underset{24}{\{5\text{-cycles}\}}$.

3-cycles still form a single conjugacy class in A_5 (because $(45) \in Z((123))$); also for $(ij)(kl)$'s ($(ij) \in Z((ij)(kl))$).
but 5-cycles split into 2 conjugacy classes in A_5.

So the class equation of A_5 is $60 = 1 + 15 + 20 + 12 + 12$.

More generally,
Prop: For $\sigma \in A_n$, $C_\sigma = \{g\sigma g^{-1} \,/\, g \in S_n\}$ splits into 2 conj. classes in A_n iff the cycle lengths of σ are all odd and distinct.

Pf: • σ commutes with the cycles in its own cycle decomposition. So any even length cycle in σ gives an odd permutation in $Z(\sigma)$ $\Rightarrow$ C_σ not split.

• if two odd cycles $(a_1 \dots a_k)$ and $(b_1 \dots b_k)$ of the same length appear in the cycle decomposition of σ, then $(a_1 b_1)(a_2 b_2)\dots(a_k b_k) \in Z(\sigma)$ odd. (this includes the case $k=1$! can't have 2 fixed points).

• if cycle lengths are all distinct, then an element of $Z(\sigma)$ must preserve each of the corresponding subsets of $\{1..n\}$; now, on a j-element subset: $Z((1\,2\dots j)) = \{$cyclic subgroup of S_j gen^d by $(1\,2\dots j)\} \subset A_j$.

So $Z(\sigma) \subset A_n$. □

Now: the class equation of A_5 is $60 = 1 + 15 + 20 + 12 + 12$.

Can now look for normal subgroups of A_5. Can't reach a divisor of 60 in any nontrivial way as a union of conj classes including $\{id\}$, except by taking all. Hence:

Prop: A_5 is simple, ie. its only normal subgroups are $\{id\}$ and itself.

Theorem: A_n is simple $\forall n \geq 5$.

A_5 just seen; A_6 similar argument using class equation (on HW 9)! However the result is false for A_4 ($\{id\} \cup \{(ij)(kl)\} \subset A_4$ is normal). The general case relies on:

Lemma: A_n is generated by 3-cycles.

Pf: Induction on n: this is true for $A_3 = \{id, \text{3-cycles}\} \subset S_3$.
Now assume A_{n-1} is generated by 3-cycles. Let $\sigma \in A_n$: if $\sigma(n) = n$ then it belongs to a subgroup $\{\tau \in A_n / \tau(n) = n\} \simeq A_{n-1}$ so it's a product of 3-cycles by induction hypothesis. Else: let $i = \sigma(n)$ and j = any element distinct from i and n, then $\tau = (j\,i\,n)\,\sigma \in A_n$ and $\tau(n) = n$, so by induction hyp. $\tau = \prod(\text{3-cycles})$, and so is $\sigma = (i\,j\,n)\,\tau$. □

* Moreover: for $n \geq 5$, 3-cycles form a single conjugacy class in A_n, since $(j_1 j_2 j_3)$ and $(k_1 k_2 k_3)$ are conjugate by any permutation $j_i \mapsto k_i$, & some of these $\in A_n$. So: to prove that a normal subgroup $H \subset A_n$, $H \neq \{e\}$ is all of A_n, it suffices to show that it contains a 3-cycle.

Proof of theorem: Let $H \subset A_n$, $H \neq \{e\}$ normal subgroup. As just noted, it's enough to show that H contains a 3-cycle. (hence all 3-cycles by conjugation, hence $H = A_n$)

- Let $\sigma \in H$, $\sigma \neq e$. Replacing σ by some power of σ, we can assume that it has prime order: let $m = \text{order}(\sigma)$, p prime $| m$, then $\sigma^{m/p} \in H$ has order p.
Since the order of σ is the l.c.m. of its cycle lengths, this implies σ is a product of disjoint p-cycles. We now look at cases depending on p:

1) If $p \geq 5$: $\sigma = (i_1 \dots i_p)\tau$, τ fixes $i_1 \dots i_p$ and permutes the remaining elements.
Then let $g = (i_4\, i_3\, i_2)$, then H normal $\Rightarrow$ $g\sigma g^{-1}$ and $g\sigma g^{-1}\sigma^{-1} \in H$.

$$g\sigma g^{-1}\sigma^{-1} = (i_4\, i_3\, i_2) \circ [(i_1 i_2 i_3 i_4 i_5 \dots i_p)\tau] \circ (i_2\, i_3\, i_4) \circ (\tau^{-1}(i_p \dots i_5 i_4 i_3 i_2 i_1))$$

takes
$$\begin{array}{l} i_1 \underset{\sigma^{-1}}{\longmapsto} i_p \underset{g^{-1}}{\longmapsto} i_p \underset{\sigma}{\longmapsto} i_1 \underset{g}{\longmapsto} i_1 \\ i_2 \mapsto i_1 \mapsto i_1 \mapsto i_2 \mapsto i_4 \\ i_3 \mapsto i_2 \mapsto i_3 \mapsto i_4 \mapsto i_3 \\ i_4 \mapsto i_3 \mapsto i_4 \mapsto i_5 \mapsto i_5 \\ i_5 \mapsto i_4 \mapsto i_2 \mapsto i_3 \mapsto i_2 \end{array}$$

$= (i_2\, i_4\, i_5)$

$\Rightarrow$ H contains a 3-cycle.

2) $p = 3$; if σ is a 3-cycle we're done. Else product of at least two disjoint 3-cycles: write $\sigma = (i_1\, i_2\, i_3)(i_4\, i_5\, i_6)\tau$, let $g = (i_4\, i_3\, i_2)$,
we find $g\sigma g^{-1}\sigma^{-1} = (i_1\, i_5\, i_2\, i_4\, i_3)$ is a 5-cycle $\in H$, this reduces to the previous case. ✓

3) $p = 2$, and σ is a product of only 2 transpositions (a single $(ij) \notin A_n$!)
$\sigma = (i_1\, i_2)(i_3\, i_4)$; let $i_5 \notin \{i_1 .. i_4\}$ and $g = (i_5\, i_3\, i_1)$.
Then $g\sigma g^{-1}\sigma^{-1} = (i_1\, i_5\, i_2\, i_4\, i_3) \in H$, back to first case.

4) $p = 2$ and σ is a product of at least 3 transpositions (in fact ≥ 4):
$\sigma = (i_1\, i_2)(i_3\, i_4)(i_5\, i_6)\tau$. Again let $g = (i_5\, i_3\, i_1)$, then
$g\sigma g^{-1}\sigma^{-1} = (i_1\, i_5\, i_3)(i_2\, i_4\, i_6) \in H$ has order 3, reduces to case 2. □

Our next topic, still very much related to understanding finite groups, is the <u>Sylow theorems</u>.
If $|G| = n$, and $k | n$, then in general there is no reason for G to contain an element of order k, or even a subgroup of order k. – the "converse to Lagrange's thm" fails.
<u>Ex:</u> A_4 (resp. A_5) has no subgroup of order 6 (resp. 30) – such a subgroup would be normal.
The first Sylow thm says: if $|G| = p^\ell m$, p prime, $p \nmid m$, then there exist subgroups of order p^ℓ.

Fix a prime p (which divides $|G|$) and write $|G| = p^e m$, $p \nmid m$.

Def. A subgroup $H \subset G$ of order $|H| = p^e$ is called a Sylow p-subgroup of G.

Theorems (Sylow, 1872)

1) For every prime p, a Sylow p-subgroup of G exists.
2) All Sylow p-subgroups are conjugates of each other:
   $H, H' \subset G$ p-Sylow $\Rightarrow \exists\, g \in G$ st. $H' = gHg^{-1}$
   Moreover, any subgroup $K \subset G$ with $|K|$ a power of p is contained in a Sylow p-subgroup.
3) Let s_p be the number of Sylow p-subgroups of G.
   Then $s_p \equiv 1 \mod p$, and $s_p \mid |G|$. (or equivalently, $s \mid m = \frac{|G|}{p^e}$)

Example. classify groups of order 15.

If $|G| = 15$ then there exist Sylow subgroups $H, K \subset G$ with $|H| = 3$, $|K| = 5$.

The numbers of such Sylow subgroups: $\begin{cases} s_3 \mid 5 \text{ and } s_3 \equiv 1 \mod 3 \Rightarrow s_3 = 1. \\ s_5 \mid 3 \text{ and } s_5 \equiv 1 \mod 5 \Rightarrow s_5 = 1 \end{cases}$

This implies H and K are normal! (since their conjugates gHg^{-1}, gKg^{-1} are also Sylow subgroups, but H and K are the unique such).

Using criterion coming up next time for direct products, this implies $G \simeq H \times K \simeq \mathbb{Z}/3 \times \mathbb{Z}/5 \simeq \mathbb{Z}/15$. Every group of order 15 is cyclic! $\square$