Key observation for classifying finite groups: G acts on itself by <u>conjugation</u>:

g acts by $h \mapsto ghg^{-1}$. We've seen that this does define a group homomorphism $G \to \mathrm{Aut}(G) \subset \mathrm{Perm}(G)$, so it is indeed an action.

- The orbits of this action are <u>conjugacy classes</u> in G, and the stabilizer of an element $h \in G$ is $\mathrm{Stab}(h) = \{g \in G \,/\, ghg^{-1} = h\} = \{g \in G \,/\, gh = hg\}$, the subgroup of elements which commute with h. This is called the <u>centralizer</u> of h, $Z(h) \subset G$. Note $\bigcap_{h \in G} Z(h) = Z(G)$ the center of G is the kernel of the action (ie. the subgroup of elements which act trivially)

  So: the action is trivial when G is abelian; faithful iff $Z(G) = \{e\}$.

* How does this help?

- The conjugacy classes form a partition of G, so $\boxed{|G| = \sum_{\substack{C \subset G \\ \text{conj. class}}} |C|,}$ (*)

  For each conjugacy class, $|C_h| = \dfrac{|G|}{|Z(h)|}$ divides $|G|$.

  Moreover $|C_e| = 1$ for the identity element, and $|C_h| = 1$ iff $h \in Z(G)$.

  (*) is called the <u>class equation</u> of the group G.

This is extremely useful. For example:

<u>Theorem</u>: ‖ If $|G| = p^2$ for p prime, then G must be abelian.

<u>Proof</u>:
- conjugacy classes have order $|C| \in \{1, p, p^2\}$, and $\sum |C| = p^2$.
  Thus, the number of conjugacy classes s.t. $|C| = 1$, ie. of central elements of G, must be a multiple of p. Hence $p \mid |Z(G)|$.
- $Z(G)$ is a subgroup of G, so $|Z(G)|$ divides p^2: it's p or p^2.
  If $|Z(G)| = p^2$ then G is abelian!
- Now assume $|Z(G)| = p$, and let $g \notin Z(G)$. Then g commutes with itself and with $Z(G)$, so $Z(g) \supset Z(G) \cup \{g\}$, hence $|Z(g)| > p$. But $Z(g)$ is a subgroup of G, so $|Z(g)| \mid p^2$.
  This implies $Z(g) = G$, ie. g commutes with all elements of G, ie. $g \in Z(G)$, contradiction. So $Z(G) = G$, G is abelian. □

(Hence the only groups of order p^2 up to iso are $\mathbb{Z}/p^2$ and $\mathbb{Z}/p \times \mathbb{Z}/p$).

- **Proposition:** There are exactly 5 groups of order 8 up to isom.

We know the 3 abelian ones: $\mathbb{Z}/8$, $\mathbb{Z}/2\times\mathbb{Z}/4$, $(\mathbb{Z}/2)^3$.

We know D_4 = symmetries of the square.

Finally: quaternion group $\{\pm 1, \pm i, \pm j, \pm k\}$ with $i^2=j^2=k^2=-1$, $ij=k$, $jk=i$, $ki=j$ (mult by -1 flips signs)

Two ways to show there's only two nonabelian groups of order 8:

- "by hand" - see HW hint: if $|G|=8$ and G not abelian.
  Step 1: a group where every element has $g^2=1$ must be abelian, so there must be an element a of order 4 (order 8 would make $G\simeq\mathbb{Z}/8$)
  Step 2: the order 4 subgroup generated by a is normal. Work out possibilities for mult. by an element b such that $ab\neq ba$.

- using conjugacy and class equation:
  Step 1: class equation $8=\sum|C|$, $|C|\in\{1,2,4,8\}$, $|C_e|=1$
  $\Rightarrow Z(G)=\{g \mid |C_g|=1\}$ has order 2, 4, or 8. $8\Rightarrow G$ abelian.
  4 is impossible by same argument as for p^2 above. So $|Z(G)|=2$.
  Step 2: if $g\notin Z(G)$ then $Z(g)\subsetneq G$, but $Z(G)\cup\{g\}\subset Z(g)$. So $|Z(g)|=4$, and $|C_g|=2$. Hence class equation is $8=\underbrace{1+1}_{e\text{ and the other central element}}+\underbrace{2+2+2}_{3\text{ other conj. classes}}$

  Then work out the possibilities!

Conjugacy classes in the symmetric group S_n:

- A k-cycle $\sigma=(a_1\,a_2\,\dots\,a_k)\in S_n$ is a permutation mapping $a_1\mapsto a_2$, $a_2\mapsto a_3$, $\dots$, $a_k\mapsto a_1$ and all other elements to themselves.
  ↳ distinct elements of $\{1..n\}$
- Two cycles are disjoint if the subsets of elements they cycle are disjoint.
  Disjoint cycles commute.
- **Prop:** any permutation can be expressed as a product of disjoint cycles, uniquely up to reordering the factors (disjoint cycles commute so order doesn't matter)

Algorithm: look at successive images of 1 under σ, this gives a subset of elements that are cyclically permuted by σ. Then consider elements not in this subset, and repeat.
In other terms: the various cycles are the restrictions of σ to the orbits of $\langle\sigma\rangle\subset S_n$ on $\{1..n\}$.

Ex: $\sigma=\begin{pmatrix}1&2&3&4&5&6\\ \downarrow&\downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\ 3&5&6&4&2&1\end{pmatrix}=(1\,3\,6)(2\,5)$ ↳ same for other elements not in the previous cycles.
↳ successive images of 1 under σ until returns to 1

Prop: Let $\sigma = (a_1 \dots a_k)$ k-cycle, $\tau \in S_n$ any permutation, then $\tau\sigma\tau^{-1} = (\tau(a_1) \dots \tau(a_k))$.

Pf: calculate: $\tau(a_i) \mapsto a_i \mapsto a_{i+1} \mapsto \tau(a_{i+1})$, so action on $\{\tau(a_i)\}$ is as claimed.
other elements $\tau(b) \mapsto b \mapsto b \mapsto \tau(b)$.

Corollary: All k-cycles are conjugate in S_n.
More generally, $\sigma, \tau \in S_n$ are conjugate iff they have the same cycle lengths in their disjoint cycle decompositions.
Hence, conjugacy classes in S_n correspond to <u>partitions of n</u>
ie. ways to write n as sum of positive integers (up to reordering the terms).

Ex: $n=3$, partitions are

$3=1+1+1$	identity	(only "1-cycles")	$\lvert$conj. class$\rvert = 1$
$3=2+1$	transpositions	(ij)	3
$3=3$	3-cycles		2

Ex: $n=4$:

partition	description	size of conj. class
$1+1+1+1$	id	1
$2+1+1$	transposition	6
$2+2$	2 transpositions	3
$3+1$	3-cycle	8
4	4-cycle	6

The class equation of S_4 is $24 = 1+3+6+6+8$.

This helps us find normal subgroups of S_4: $H \subset G$ normal iff $aHa^{-1} = H \ \forall a \in G$
So a normal subgroup is a union of conjugacy classes! Also, must include id, and $|H|$ divides $|G|$. Here: apart from $\{id\}$ and S_4, the only candidates are

$1+3 = 4 \mid 24$: $\{id\} \cup \{(ij)(kl)\}$. This is indeed a normal subgp. ($\simeq \mathbb{Z}/2 \times \mathbb{Z}/2$)

$1+3+8 = 12 \mid 24$: $\{id\} \cup \{(ij)(kl)\} \cup \{3\text{-cycles}\}$. This is the alternating gp $A_4 < S_4$

Ex: $n=5$:

partition	description	size of conj. class
$1+1+1+1+1$	id	1
$2+1+1+1$	transposition	10
$2+2+1$	2 transpositions	15
$3+1+1$	3-cycle	20
$3+2$	3-cycle + transposition	20
$4+1$	4-cycle	30
5	5-cycle	24

Class equation: $120 = 1 + 10 + 15 + 20 + 20 + 24 + 30$.

Search for normal subgroups (besides $\{id\}$ and S_5):

only options are $1 + 15 + 24 = 40$ $\quad \{id\} \cup \{(ij)(kl)\} \cup \{5\text{-cycles}\}$

This is not a subgroup, $(12345)(12)(34) = (135)$

and $\underbrace{1 + 15 + 20 + 24}_{2 \text{ possibilities}} = 60$: id, $(ij)(kl)$, 5-cycles, and either 3-cycles or (3-cycle)(transposition)

By the above, only the first option (3-cycles) works, & gives $A_5 \subset S_5$.

The alternating group:

Recall we've defined the sign homomorphism $S_n \to \{\pm 1\}$ by $\operatorname{sgn}(\prod_{i=1}^{k} \text{transpositions}) = (-1)^k$ using that transpositions generate S_n; still need to check this is independent of how we express σ as a product of transpositions. I mentioned: $\operatorname{sgn}(\sigma) = (-1)^{\text{inversions}}$ where inversions $= \{(i,j) \mid 1 \le i < j \le n \text{ and } \sigma(i) > \sigma(j)\}$. (but then... check it's a homomorphism?).

Now we can do better:

take a vector space $V \simeq \mathbb{R}^n$, with basis $(e_1, \dots, e_n)$, then to each $\sigma \in S_n$ we associate an element of $GL(V) = GL(n)$: the linear map $T_\sigma : V \to V$ s.t. $e_i \mapsto e_{\sigma(i)}$. This gives an injective homomorphism $S_n \hookrightarrow GL(n)$ (with image the subgroup of "permutation matrices")

Now, T_σ has finite order (since σ does) hence $\det(T_\sigma) \in \mathbb{R}$ is a root of unity, hence $\in \{\pm 1\}$. Can define $\operatorname{sgn}(\sigma) = \det(T_\sigma)$ - clearly well def.^d^ and homomorphism.

Concretely, to compute the sign: $\Lambda^n T_\sigma$ acts on $\Lambda^n V$ by $e_1 \wedge \dots \wedge e_n \mapsto e_{\sigma(1)} \wedge \dots \wedge e_{\sigma(n)}$ and the sign is the number of transpositions needed to switch these back in order, so this agrees with the other def.^n^.

* 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 if $\sigma \in S_n$ has cycle lengths $k_1, \dots, k_\ell$ (incl. the 1's) ie. corresponds to partition $n = k_1 + \dots + k_\ell$, then $\operatorname{sgn}(\sigma) = (-1)^{\sum (k_i - 1)} = (-1)^{n-\ell}$.

Def: $A_n = \ker(\operatorname{sgn}) \subset S_n$ (a normal subgroup of index 2 in S_n). the alternating group.

* Prop: If $C \subset S_n$ is a conjugacy class then either (1) C is odd, $C \cap A_n = \phi$, or (2a) $C \subset A_n$ is a conjugacy class in A_n, (2b) $C \subset A_n$ splits into 2 conjugacy classes in A_n.

Case 2a vs. 2b: $\sigma \in C$, $Z(\sigma) = \{\tau \in S_n \,/\, \tau\sigma\tau^{-1} = \sigma\}$ centralizer,

is $Z(\sigma) \subset A_n$ or not? if yes then conjugates of σ by odd permutations are different from conjugates by even permutations, form two conj. classes in A_n.

if not then all conjugates of σ in S_n are conjugate by elements of A_n.

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

3-cycles still form a single conjugacy class in A_5; also for $(ij)(kl)$'s

(because $(45) \in Z((123))$) $\qquad$ $((ij) \in Z((ij)(kl)))$.

5-cycles split into 2 conjugacy classes in A_5.

So 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, hence only $\{1\}$ and A_5:

$\Rightarrow$ Prop: A_5 is simple.