30) Consider a group $G \leq S_6$ of permutations of 6 points. This group also acts on sets of size 2. You are given the information that $(2,6,5,3)$, $(1,6,2)(3,5,4)$ are the (only) permutations in G that map the set $\{1,2\}$ to $\{1,6\}$. (So they form a coset of $\mathrm{Stab}_G(\{1,2\})$.) Using the fact that $\mu(\{1,6\},(2,6,5,3)) = \{1,5\}$, determine the set of all permutations of G that map $\{1,2\}$ to $\{1,5\}$.

31) Let $G = \left\langle \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \right\rangle$ with multiplication done modulo 2. (In fact $G = \mathrm{GL}_3(2)$, but you do not need to show this.)

a) G acts by right multiplication on the $2^3 = 8$ vectors of length 3. Calculate the orbits.

b) Show that the stabilizer of the vector $(1,0,0)$ (row vector, arithmetic again done modulo 2) must consist of matrices of the form $\begin{pmatrix} 1 & 0 & 0 \\ a & b & c \\ d & e & f \end{pmatrix}$. Conclude that the condition of invertibility requires that the submatrix $\begin{pmatrix} b & c \\ e & f \end{pmatrix}$ must have determinant 1 (modulo 2) and thus must lie in $\mathrm{GL}_2(2)$, but that a and b can be chosen freely (as 1 or 0).

c) From class we know that there are 6 possible submatrices $\begin{pmatrix} b & c \\ e & f \end{pmatrix}$, using this, explain that $\mathrm{Stab}_G((1,0,0))$ must have order 24.

d) Calculate $|G|$.

e) Write down a permutation for the first generator of G that describe the action of G on the orbit of $(1,0,0)$.

32) We know that the group G of rotational symmetries of a dodecahedron has 60 elements.

a) Using that rotations are centered at a face, a corner or an edge, calculate the distribution (i.e. 1 of order 1, 1 of order 2, …) of element orders in G.

b) If p is a prime, show that a (cyclic) group of order p has 1 element of order 1 and $p-1$ elements of order p, and that two different cyclic subgroups of order p will have an intersection of size 1.

c) Using the numbers from a) and the result of b), How many subgroups of order 3, and how many subgroups of order 5 does G have?

33) Let G be a group, acting on a set Ω and $g, h \in G$.

a) Show that if $\omega, \delta \in \Omega$ such that g maps ω to δ, that $h^{-1}gh$ maps ω^h to δ^h.

b) Show that if $S = \mathrm{Stab}_G(\omega)$, the subgroup $S^h = h^{-1}Sh$ is the stabilizer of ω^h.

c) Considering the special case of $G = S_n$ and $\omega = \{1,\ldots,n\}$, conclude from a) that the cycle structure of g must equal that of h^-1gh.

d) Let $G = S_n$ and $x, y \in G$ with the same cycle structure. Show that there exists h^G such that $h^{-1}xh = y$. (Note: This does not hold for proper subgroups!)

34) (Continuation of problem 33 b) Let G be a finite group and $H \leq G$. We consider the action of G on the cosets of H by right multiplication $\mu(Hx, g) = H(xg)$. Show that the kernel of this action is $\bigcap_{g \in G} H^g$ (where $H^g = g^{-1}Hg$).

35) (Continuation of problem 33 c) **a)** The German "Enigma" encryption machine, used in the second world war, produced (by a set of moving rotors) in each step a permutation $\sigma \in S_{26}$ that was use to scramble letters (interpreting the numbers 1-26 as letters in the alphabet) in a different way each step.
Show that it is not always possible to use the *same* setting (i.e. the same permutation σ) to encrypt and decrypt.

b) To ease handling for the operators (who understood little math) and avoid confusion with separate *encrypt/decrypt* settings, the German military had the "clever" idea to add a "plug-board" (on the picture in front of the machine) that swapped pairs of letters (this creates a permutation π that has a cycle type as $(1,2)(3,4)(5,6)\cdots(25,26)$) and to feed the encryption through the old mechanism (σ), then through the plug-board, and in reverse back through the mechanism. So the encryption performed now was of the form $\mu = \sigma^{-1}\pi\sigma$.
Show that this encryption is self-reverting, i.e. that $\mu^2 = 1$. (Thus the same setting could be used for encryption and decryption.)

c) How many possibile permutations $\sigma \in S_n$ exist? How many possible permutation $\mu = \sigma^{-1}\pi\sigma$ exists? Explain, based on this count, why the "clever" idea was really stupid (and indeed was one of the reasons the code could be broken).