Precall that a group $G$ is called cyclic if there is an element $g \in G$ such that

every element of $G$ is a power of $g$:

$$G = \{1, g, g^2, g^3, \ldots \}.$$

(a) Show that if $G$ is cyclic and $H$ is a subgroup of $G$ then $H$ is cyclic. Hint:
Let $k$ be the least positive integer such that $g^k \in H$. If $g^l$ is any other
element of $H$ then $k \mid l$; otherwise by long division we can write $l = qk + r$
for some $0 < r < k$, so...

(b) Consider a Rubik’s cube. You might hope there is some clever sequence of
moves such that if you take any mixed-up cube and make this sequence of
moves over and over, you will eventually get to the “solved” position, no
matter where you started. Show that this is not the case by observing that
the symmetry group $G$ of the Rubik’s cube contains a copy of $\mathbb{Z}_4 \times \mathbb{Z}_4$,
given by rotating the top and the bottom, and this is not a cyclic group.

2. Let $S_n$ denote the symmetric group on $n$ letters.

(a) Show that an $m$-cycle $(a_1 a_2 \cdots a_m)$ is an even permutation if and only
if $m$ is odd. Hint: The point is just to remember how to factor $\sigma$ as a
product of transpositions.

(b) Let $A_n \subset S_n$ be the subgroup of even permutations; then the order of $A_n$
is half that of $S_n$. Why?

(c) List the 12 elements of $A_4$, in cycle notation.

(d) Let $A_4$ act on itself by conjugation. How many orbits are there? How
many elements are in each orbit? Hint: To save time, it is enough to see how
$(1 \, 2)(3 \, 4)$, $(1 \, 3)(2 \, 4)$, and $(1 \, 4)(2 \, 3)$ act on the 3-cycles, and
how $(1 \, 2 \, 3)$ acts on the products of 2-cycles; then note that conjugation
preserves cycle type, and there is no orbit of order eight (why?), so the
orbits can’t get any bigger than what you’ve already found at this point.
Further hint: If this is taking you forever, go work on another problem
and maybe come back later.

*There is an algorithm for solving the Rubik’s cube, but it is not as simple as “make this sequence of moves over and over.”
3. Let $R$ be a ring and $S$ a subring. Show that if $I$ is an ideal of $R$ then $J = I \cap S$ is an ideal of $S$. Show that if $I$ is a prime ideal of $R$ then $J$ is a prime ideal of $S$.

4. Let $S = \mathbb{Z} [\sqrt{-3}]$, and let $R = \mathbb{Z}[\omega]$, where $\omega = e^{2\pi i/3} = \frac{-1 + \sqrt{-3}}{2}$ is a cube root of unity. Observe that $\sqrt{-3} = 2\omega + 1$, so $S$ is a subring of $R$, and that both are subrings of $\mathbb{C}$ and thus in particular integral domains. Here is a picture of $R$, with the subring $S$ shown in heavier dots:

(a) Observe that if $z = a + b\sqrt{-3} \in S$ then $|z|^2 = a^2 + 3b^2$, which is a non-negative integer for all $a, b \in \mathbb{Z}$. Conclude that $z$ is a unit in $S$ if and only if $|z| = 1$. List the units in $S$. Hint: There are two.

(b) Observe that if $z = a + b\omega \in R$ then $|z|^2 = a^2 - ab + b^2$, which is a non-negative integer for all $a, b \in \mathbb{Z}$: non-negative because it’s $|z|^2$, and an integer because it’s $a^2 - ab + b^2$. Conclude that $z$ is a unit in $R$ if and only if $|z| = 1$. List the units in $R$. Hint: There are six.

(c) Show that 2 is irreducible in $S$. Hint: Argue that there is no $z \in S$ with $|z|^2 = 2$. Thus if $2 = zw$ then . . .

(d) Observe that $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$. Conclude that 2 is not prime in $S$.

(e) I was going to ask you to show that 2 is prime (and hence irreducible) in $R$, but this turns out to be a pain.

(f) Show that the ideals generated by 2 and $1 - \sqrt{-3}$ in $R$ are the same, but that the ideals they generate in $S$ are different. Hint: Recall from homework that $(a) = (b)$ if and only if there is a unit $u$ such that $a = ub$. Warning: Consider writing $(2)_R$ and $(2)_S$ rather than just $(2)$ to avoid confusion.

(g) Let $I = (2)_R \subset R$ and $J = I \cap S$. Show that $J = (2, 1 - \sqrt{-3})_S$, and that this is not a principal ideal. Hint: It is clear that $2 \in I \cap S$ and $1 - \sqrt{-3} \in I \cap S$; for the reverse containment, note that a general element of $I$ is of the form $2(a + b\omega)$, and multiply that out.