Exercise 1. Show that the order of an element in S_n equals the least common multiple of lengths of the cycles in its cycle decomposition. (You may use the result from Exercise 1 in Homework 2.) 1.3.15

Solution. Consider an element $\sigma \in S_n$ and suppose that its cycle decomposition is $\sigma = \tau_1 \dots \tau_k$ (including 1-cycles), and each τ_t is an m_t-cycle for $1 \leq t \leq k$. Then the cycles partition the set of elements $\{1, \dots, n\}$ such that every element $x \in \{1, \dots, n\}$ is in exactly one τ_t for $1 \leq t \leq k$. Therefore $\sigma(x) = \tau_t(x)$. By Exercise 1 in Homework 2, we have that $\sigma^i(x) = \tau_t^i(x) = x$ if and only if m_t divides i. Therefore $\sigma^i = 1$ if and only if m_t divides i for all $1 \leq t \leq k$. Then, $|\sigma|$ is the least natural number with that property, i.e. the least common multiple of $m_1, \dots, m_k$.

Exercise 2. Find all the numbers n such that S_6 contains and element of order n. 1.3.18

Solution. Using the previous exercise, we see that, to determine the order of an element, all we need to know is the set of cycle lengths in its disjoint cycle notation. Note that in this form, the lengths of the cycles add up to 6 always (if we include the length 1 cycles). These are called integer partitions of 6, and we will see more of this later on. This gives us the following orders:

Cycle lengths	LCM
6	6
$5, 1$	5
$4, 2$	4
$4, 1, 1$	4
$3, 3$	3
$3, 2, 1$	6
$3, 1, 1, 1$	3
$2, 2, 2$	2
$2, 2, 1, 1$	2
$2, 1, 1, 1, 1$	2
$1, 1, 1, 1, 1, 1$	1

Therefore, the possible orders of elements in S_6 are 1, 2, 3, 4, 5, 6.

Exercise 3. Show that if $\phi : G \to H$ is a homomorphism, then we must have that $\phi(1) = 1'$, where 1 is the identity of G and $1'$ the identity of H.

Solution. Note that we already proved this in Exercise 2 of Homework 2 (equivalent to the case $n = 0$). Here is an alternative proof.
We know that if ϕ is a homomorphism, then $\phi(a)\phi(b) = \phi(ab)$ in H for any $a, b \in G$. Therefore, for any $a \in G$, we have that

$$\phi(1)\phi(a) = \phi(1a) = \phi(a).$$

If we multiply this on both sides by $\phi(a)^{-1}$, we obtain

$$\phi(1)\phi(a)\phi(a)^{-1} = \phi(1) = \phi(a)\phi(a)^{-1} = 1',$$

which shows that $\phi(1) = 1'$.

Exercise 4. Show that the additive groups $\mathbb{Z}$ and $3\mathbb{Z}$ are isomorphic.

Solution. One way to show that two groups are isomorphic is to find a bijective homomorphism between the two. We let $\phi : \mathbb{Z} \to 3\mathbb{Z}$ be given by $\phi(n) = 3n$ for all $n \in \mathbb{Z}$. We see that this map is bijective by noting that every element in $3\mathbb{Z}$ can be written as $3k$, with $k \in Z$, and therefore $\phi^{-1}(m) = m/3$ is the inverse function that maps $3\mathbb{Z}$ back to $\mathbb{Z}$.

We still need to show that ϕ is indeed a homomorphism. For any $i, j \in \mathbb{Z}$, we have $\phi(i+j) = 3(i+j) = 3i + 3j = \phi(i) + \phi(j)$, as needed.

Exercise 5. Prove that a group G acts faithfully on a set A if and only if the kernel of the action is the set consisting only of the identity. 1.7.6

Solution. We need to prove both directions of this bidirectional statement.

- $\Rightarrow$ Suppose that G acts faithfully on a set A, and for the sake of contradiction, suppose that we have an element $1 \neq g \in \ker \cdot$. Let $h \in G$. Then the two elements h and hg must be distinct. We have

  $$h \cdot a = h \cdot (g \cdot a) = (hg) \cdot a, \text{ for all } a \in A.$$

  This is a contradiction, since a faithful action implies that $\sigma_h \neq \sigma_{hg}$ when $h \neq hg$.

- $\Leftarrow$ Suppose that $\ker \cdot = \{1\}$, and, for the sake of contradiction, that there are two distinct elements $h \neq g$ in G such that $\sigma_h = \sigma_g$. We let $k = g^{-1}h$ such that we can write $h = gk$. Note that since $h \neq g$ we have $k \neq 1$. We have

  $$g \cdot a = h \cdot a = (gk) \cdot a = g \cdot (k \cdot a), \text{ for all } a \in A.$$

  Since $g \cdot a$ induces a permutation on the set a, we have that $g \cdot a = g \cdot b$ implies that $a = b$. Therefore, we can read the equation above as

  $$a = k \cdot a, \text{ for all } a \in A.$$

  However, this implies that $k \in \ker \cdot$, which is a contradiction.

Exercise 6. Asssume n is an even positive integer and show that D_{2n} acts on the set consisting of pairs of opposite vertices of a regular n-gon. Find the kernel of this action. 1.7.12

Solution. When we view the action of D_{2n} on a regular n-gon as the rigid motions of the n-gon, we see that pairs of opposite vertices stay opposite vertices. Vertex a being opposite vertex b is a property of the n-gon itself, not of its orientation in space. And, since vertices are permuted by this action, we see that pairs must in fact also be permuted.

To examine this more closely, we'll label the vertices $1, \ldots, n$ where $2k = n$ (since n is even). Then opposite pairs look like $\{i, i+k \pmod{()n}\}$. From now on $\pmod{n}$ will be assumed. From the example of the checkerboard-colored square that we did in class, we saw that the kernel of that action was $\{1, r^2, sr, sr^3\}$. Now, let $n \geq 6$. If r is the rotation clockwise over $\frac{360^\circ}{n}$, then r^t sends i to $i+t$. Therefore, the only rotations that preserves opposite pairs are the 0° rotation the element 1 and the 180° rotation (the element r^k), which swaps vertices within each pair but preserves the pairs. For the reflections, consider first the reflection through an axis of symmetry that passes through opposite vertices $i, i+k$. This reflection exhanges the pairs $\{i-1, i+k-1\}$ and $\{i+1, i+k+1\}$, and is therefore not an identity permutation. Similarly, consider the reflection through an axis of symmetry that passes through the middle of two opposite edges $(i, i+1)$ and $(i+k, i+k+1)$. This reflection exhanges the pairs $\{i, i+k\}$ and $\{i+1, i+k+1\}$, and is therefore not an identity permutation. Therefore, the kernel of any such action when $n \geq 6$ is $\{1, r^k\}$.