1. Symmetric groups and cyclic groups.

It is convenient to have a way of describing individual elements in symmetric groups. Here is a good way to do that: let \( n \) be a positive integer, and let \( \Sigma_n \) be the symmetric group on \( n \) symbols. Remember that this means that \( \Sigma_n \) is the group of symmetries of a set with \( n \) elements. Let’s choose a particular set with \( n \) elements, namely, the set of positive integers less than or equal to \( n \). Now suppose \( f \in \Sigma_n \), and let \( i \) be an integer, \( 1 \leq i \leq n \). Then \( f(i) \) is some integer between 1 and \( n \), and \( f(f(i)) \) is some integer between 1 and \( n \), and so on. I will write \( f^j \) for the \( j \)-fold composite of \( f \) with itself, so for example, \( f^3(i) = f(f(f(i))) \).

I claim that there exists some integer \( k \) such that \( f^k(i) = i \). Here is a proof of this claim: since there are only finitely many integers between 1 and \( n \), it cannot be the case that \( i, f(i), f^2(i), f^3(i), f^4(i), \ldots \) are all distinct. So there must be some pair of integers \( \ell, m \) such that \( \ell < m \) and such that \( f^{\ell}(i) = f^m(i) \). But \( f \) is a one-to-one correspondence, so there exists an inverse function \( f^{-1} \) to \( f \). Let \( f^{-\ell} \) denote the \( \ell \)-fold composite of \( f^{-1} \) with itself. Then applying \( f^{-\ell} \) to the equality \( f^{\ell}(i) = f^m(i) \), we get

\[
\begin{align*}
  i &= f^{-\ell}(f^{\ell}(i)) \\
  &= f^{-\ell}(f^m(i)) \\
  &= f^{m-\ell}(i).
\end{align*}
\]

So \( m - \ell \) is the desired integer \( k \) such that \( f^k(i) = i \).

Here is the practical consequence of knowing that there exists some integer \( k \) such that \( f^k(i) = i \): we can write down the cycle of \( i \) under repeated iteration of \( i \), that is, we can write down the sequence

\[
i, f(i), f(f(i)), \ldots
\]

and we can be assured that this sequence eventually “loops back around” to \( i \), so we only need record a finite amount of information. Note that, if we write down the cycle of each integer \( i \in \{1, \ldots, n\} \), then this information uniquely determines the element \( f \in \Sigma_n \); and note also that, if we write down the cycle of \( i \), it is not necessary to write down the cycle of \( f(i) \), since \( f(i) \) and \( i \) have exactly the same sequence of numbers in their cycle.

Examples are the way to make this clear. Let’s look at \( \Sigma_4 \), the group of symmetries of the set \( \{1, 2, 3, 4\} \). One good example of an element of \( \Sigma_4 \) is the element \( \sigma \in \Sigma_4 \) defined as follows: \( \sigma(i) = i + 1 \) if \( i < 4 \), and \( \sigma(4) = 1 \). In other words, \( \sigma \) “rotates everything one spot to the right.” Then the cycle decomposition of \( \sigma \) is written \((1234)\).

Let’s also look at the element \( \tau \in \Sigma_4 \) defined by \( \tau(1) = 2 \) and \( \tau(2) = 1 \) and \( \tau(3) = 3 \) and \( \tau(4) \). Then the cycle decomposition of \( \tau \) is written \((12)\), since \( \tau \) swaps 1 and 2, and does nothing to 3 and 4; when a number \( i \) is fixed by an element \( f \in \Sigma_n \), i.e., the cycle of \( i \) is just \( (i) \), by convention we do not write \( (i) \) in the cycle decomposition of \( f \).

Date: September 2015.
What happens if we take the composite \( \sigma \circ \tau \)? That’s an element of \( \Sigma_4 \). Let’s compute its cycle decomposition:

\[
\begin{align*}
\sigma(\tau(1)) &= \sigma(2) = 3, \\
\sigma(\tau(2)) &= \sigma(1) = 2, \\
\sigma(\tau(3)) &= \sigma(3) = 4, \\
\sigma(\tau(4)) &= \sigma(4) = 1.
\end{align*}
\]

So the cycle decomposition of \( \sigma \circ \tau \) is \((134)\).

What if we are given two elements of \( \Sigma_n \) in terms of their cycle decompositions, and we have to compose them? This is easily handled: suppose we want to compose \((34)\) and \((123)\). We simply see what the composite does to each integer \(i = 1, 2, 3, 4\):

\[
\begin{align*}
(34) \circ (123) &\text{ sends } 1 \text{ to } 2, \\
(34) \circ (123) &\text{ sends } 2 \text{ to } 4, \\
(34) \circ (123) &\text{ sends } 3 \text{ to } 1, \\
(34) \circ (123) &\text{ sends } 4 \text{ to } 3.
\end{align*}
\]

So \((34)(123) = (1243)\).

These cycle decompositions are a convenient, compact way to describe individual elements of \( \Sigma_n \), and you are likely to find cycle decompositions useful in the homework exercises.

**Definition 1.1.** Suppose \( G \) is a finite group. The order of \( G \) is the number of elements of \( G \).

Suppose that \( g \in G \). The order of \( g \) is the least integer \( n \) such that \( g^n = 1 \). If \( G \) is an infinite group, then for some elements \( g \in G \), there may be no such integer \( n \); in that case, we say that \( g \) has infinite order.

**Definition 1.2.** We say that a group \( G \) is cyclic if \( G \) can be generated by a single element, i.e., there exists some element \( g \in G \) such that every element in \( G \) is of the form \( g^n \) for some integer \( n \).

We write \( \mathbb{Z} \) for the unique (up to isomorphism) infinite cyclic group, that is, \( \mathbb{Z} \) is the group of integers under addition, or equivalently, \( \mathbb{Z} \) is the free group on one generator. If \( n \) is a positive integer, we write \( \mathbb{Z}/n\mathbb{Z} \) for the group of integers under addition modulo \( n \).

So, for example, \( \mathbb{Z}/3\mathbb{Z} \) is the abelian group with elements \( \{0, 1, 2\} \), with group operation given by

\[
\begin{align*}
0 + 0 &= 0, \\
0 + 1 &= 1, \\
0 + 2 &= 2, \\
1 + 0 &= 1, \\
1 + 1 &= 2, \\
1 + 2 &= 0, \\
2 + 0 &= 2, \\
2 + 1 &= 0, \\
2 + 2 &= 1.
\end{align*}
\]
This is just the elementary addition modulo 3 (i.e., add two numbers and take the remainder after dividing by 3) which you learned to do many, many years ago. Section 0.3 in your textbook has a nice recap of the basic properties of \( \mathbb{Z}/n\mathbb{Z} \), which you might find helpful.

**Exercise 1.3. (Easy.)** Prove that every cyclic group is abelian.

**Exercise 1.4. (Also easy.)** Prove that every cyclic group is isomorphic to either \( \mathbb{Z} \) or \( \mathbb{Z}/n\mathbb{Z} \) for some positive integer \( n \).

**Exercise 1.5. (Also easy.)** Suppose that \( n > 2 \). Prove that the symmetric group \( \Sigma_n \) is not cyclic.

**Definition 1.6.** The Euler \( \phi \)-function is the function from positive integers to positive integers defined as follows: \( \phi(n) \) is the number of positive integers less than \( n \) which are relatively prime to \( n \).

So, for example, \( \phi(20) = 8 \), since 1, 3, 7, 9, 11, 13, 17, and 19 are the positive integers less than 20 which do not have a factor in common with 20. Section 0.2 in your textbook has a nice exposition of some of the most basic properties of the Euler \( \phi \)-function.

**Exercise 1.7. (Also easy.)** Let \( n \) be a positive integer. Prove that there are exactly \( \phi(n) - 1 \) elements of \( \mathbb{Z}/n\mathbb{Z} \) which are of order \( n \), where \( \phi \) is the Euler \( \phi \)-function.

**Example 1.8.** Let’s compute the cyclic subgroups of \( \Sigma_3 \). Write \( \sigma \) as shorthand for the cycle (12), and write \( \tau \) as shorthand for the cycle (123). (This is consistent with the notation we used for elements of \( \Sigma_3 \) in the previous set of lecture notes.) Then:

- The unit element 1 ∈ \( \Sigma_3 \) generates a cyclic subgroup \{1\} of \( \Sigma_3 \) of order one (of course, this happens in every group, not just \( \Sigma_3 \)).
- The element \( \sigma \) satisfies \( \sigma^2 = 1 \), so \( \sigma \) generates a cyclic subgroup \{1, \sigma\} of \( \Sigma_3 \) of order two.
- The element \( \tau \) satisfies \( \tau^3 = 1 \), so \( \tau \) generates a cyclic subgroup \{1, \tau, \tau^2\} of \( \Sigma_3 \) of order three. Notice that \( \tau^2 \) generates the same subgroup of \( \Sigma_3 \), since \( (\tau^2)^2 = \tau^4 = \tau^3\tau = \tau \cdot \tau = \tau \).
- The element \( \sigma\tau \) satisfies
  \[
  (\sigma\tau)^2 = \sigma\tau\sigma\tau \\
  = \sigma\sigma\tau^2\tau \\
  = \sigma^2\tau^3 \\
  = 1 \cdot 1 \\
  = 1,
  \]
  so \( \sigma\tau \) generates a cyclic subgroup \{1, \sigma\tau\} of \( \Sigma_3 \) of order two.
- The element \( \sigma\tau^2 \) satisfies
  \[
  (\sigma\tau^2)^2 = \sigma\tau^2\sigma\tau^2 \\
  = \sigma\sigma\tau^4 \\
  = \sigma^2\tau^3 \\
  = 1 \cdot 1 \\
  = 1,
  \]
  so \( \sigma\tau^2 \) generates a cyclic subgroup \{1, \sigma\tau^2\} of \( \Sigma_3 \) of order two.

So \( \Sigma_3 \) has five cyclic subgroups: one of order 1, three of order 2, and one of order 3.
Exercise 1.9. Find all the cyclic subgroups of $\Sigma_4$.
(As you are doing this, note that this is almost the same thing as computing the order of each element of $\Sigma_4$.)

The following exercise tells you a very good reason why the symmetric groups are important:

Exercise 1.10. Prove that every finite group is isomorphic to a subgroup of a symmetric group $\Sigma_n$ for some $n$.
(Hint: this will take a bit of thought. First of all, to show that a group $H$ is isomorphic to a subgroup of another group $H'$, it suffices to construct a one-to-one group homomorphism $f : H \to H'$, since then $H$ is isomorphic to the image of $f$, which is a subgroup of $H'$. So you should try to construct a one-to-one group homomorphism from any given finite group $G$ to $\Sigma_n$ for some $n$. The trick here is to recognize that $\Sigma_n$ is the group of all one-to-one correspondences from a set with $n$ elements to itself, and given a finite group $G$, there is a way to regard $G$ as a group of some one-to-one correspondences from a certain set with $n$ elements (but what is $n$ here? It depends on $G$, but in a simple way, which you can figure out!) to itself.)

2. Dihedral groups.

Another important family of groups are the dihedral groups.

Definition 2.1. Let $n$ be an integer, $n > 2$. The dihedral group of order $2n$, written $D_{2n}$, is the group of distance-preserving, angle-preserving bijective functions from a regular polygon with $n$ sides to itself.

The dihedral groups are relatively easy to understand in many ways. For example:

Proposition 2.2. The dihedral group $D_{2n}$ has $2n$ elements.
(So the name “dihedral group of order $2n$” is an appropriate name.)

Proof. Choose a vertex of a regular polygon with $n$ sides, and starting with that vertex, label the vertices of the polygon from 1 to $n$ in clockwise order. (Counterclockwise works equally well; all that matters is to choose one direction and stick with it.) Now suppose $f \in D_{2n}$. Then $f(2)$ is some integer, $1 \leq f(2) \leq n$. Since $f$ preserves distance, $f$ must then send 1 and 3 to the two vertices adjacent to $f(2)$. There are two possibilities:

If $f(3)$ is the vertex immediately clockwise from $f(2)$: Then $f(4)$ must be one of the vertices adjacent to $f(3)$, and $f(4)$ cannot be the vertex counterclockwise from $f(3)$, since that is $f(2)$, and $f$ must be bijective, so we cannot have $f(2) = f(4)$. So, reading clockwise from $f(2)$, we have $f(2), f(3), f(4)$, and, by induction, $f(5), f(6), \ldots$, until we reach $f(n)$, and then we wrap around to $f(1)$.

It is worth it to write out the induction carefully. (You should be able to write out basic proof strategies like an induction carefully, before you start allowing yourself to skip the details in routine cases.) So here it is: suppose we have already shown that $f(i)$ is the vertex immediately clockwise from $f(i - 1)$. Then $f(i + 1)$ must be one of the vertices adjacent to $f(i)$. We cannot have $f(i + 1)$ being the vertex immediately counterclockwise from $f(i)$, since that vertex is $f(i - 1)$, and $f$ is bijective so we cannot have $f(i - 1) = f(i + 1)$. So $f(i + 1)$ must be immediately clockwise from $f(i)$. This completes the induction.

If $f(3)$ is the vertex immediately counterclockwise from $f(2)$: Then $f(4)$ must be one of the vertices adjacent to $f(3)$, and $f(4)$ cannot be the vertex clockwise from
Proposition 2.3. Let $n$ be an integer, $n > 2$. A presentation for $D_{2n}$ is:

$$D_{2n} = \langle \sigma, \tau \mid \sigma^2 = 1, \tau^n = 1, \sigma \tau = \tau^{-1} \sigma \rangle.$$ 

Proof. Number the vertices of the $n$-gon as in the proof of Proposition 2.2, and let $\sigma \in D_{2n}$ be the symmetry of the $n$-gon given by reflection about a line passing through the vertex 1 and the center of the $n$-gon, i.e., $\sigma(i) = n + 2 - i$ modulo $n$. Let $\tau$ be the symmetry of the $n$-gon given by rotation clockwise (although counterclockwise works equally well; all that is important is to choose one, and stick with it) by $\frac{2\pi}{n}$ radians. Then it is clear that $\sigma^2 = 1$ and $\tau^n = 1$. It is also clear that $\sigma$ and $\tau$ generate $D_{2n}$, since we showed (in the proof of Proposition 2.2) that an element of $D_{2n}$ can be described uniquely by describing $f(2)$ and whether $f(3)$ is immediately clockwise or immediately counterclockwise from $f(2)$, and we can arrange for $f(2)$ to be any integer between 1 and $n$ by applying the rotation $\tau$ an appropriate number of times, and we can arrange for $f(3)$ to be immediately clockwise or immediately counterclockwise from $f(2)$ by either applying the reflection $\sigma$ before rotating, or not.

The more interesting relation between $\sigma$ and $\tau$ is what happens when we compose $\sigma$ with $\tau$: we have $\sigma(\tau(i)) = \sigma(i + 1) = n + 2 - (i + 1) = n - i + 1$ modulo $n$, and we have $\tau^{n-1}(\sigma(i)) = \tau^{n-1}(n + 2 - i) = n + 2 - i - 1 = n - 1 + i$ modulo $n$. So $\sigma \tau = \tau^{n-1} \sigma$. So the subgroup of $D_{2n}$ generated by $\sigma$ and $\tau$ indeed satisfies the relations $\sigma^2 = 1$, $\tau^n = 1$, and $\sigma \tau = \tau^{n-1} \sigma$. The trick now is to show that there are no more relations between $\sigma$ and $\tau$ in $D_{2n}$. Let’s count the elements in the group $\langle \sigma, \tau \mid \sigma^2 = 1, \tau^n = 1, \sigma \tau = \tau^{n-1} \sigma \rangle$: we have

$$1, \tau, \tau^2, \ldots, \tau^{n-1},$$

and we have

$$\sigma, \tau \sigma, \tau^2 \sigma, \ldots, \tau^{n-1} \sigma,$$
Any element that has a $\sigma$ followed by a $\tau$ can be rewritten to have $\tau$ followed by $\sigma$ instead, using the relation $\sigma \tau = \tau^{n-1} \sigma$. For example:

\[
\sigma \tau^2 \sigma \tau \sigma = (\sigma \tau) \tau (\sigma \tau) \sigma \\
= (\tau^{n-1} \sigma) \tau (\tau^{n-1} \sigma) \sigma \\
= (\tau^{n-1} \sigma) \tau^n \sigma \sigma \\
= \tau^{n-1} \sigma.
\]

So $\sigma$ and $\tau$ generate both the group $D_{2n}$ and the group $\langle \sigma, \tau \mid \sigma^2 = 1, \tau^n = 1, \sigma \tau = \tau^{n-1} \sigma \rangle$, and the relations $\sigma^2 = 1, \tau^n = 1, \sigma \tau = \tau^{n-1} \sigma$ hold in both groups. The only question is whether there are any additional relations that hold in $D_{2n}$ that are not algebraic consequences of the relations $\sigma^2 = 1, \tau^n = 1, \sigma \tau = \tau^{n-1} \sigma$. But if there were additional relations in $D_{2n}$, then $D_{2n}$ would have fewer elements than the group $\langle \sigma, \tau \mid \sigma^2 = 1, \tau^n = 1, \sigma \tau = \tau^{n-1} \sigma \rangle$; but we already have seen that both $D_{2n}$ and $\langle \sigma, \tau \mid \sigma^2 = 1, \tau^n = 1, \sigma \tau = \tau^{n-1} \sigma \rangle$ each have $2n$ elements, the same number. Hence $D_{2n} = \langle \sigma, \tau \mid \sigma^2 = 1, \tau^n = 1, \sigma \tau = \tau^{n-1} \sigma \rangle$. \hfill \Box

**Exercise 2.4.** (Very easy.) Prove that $D_6$ is isomorphic to $\Sigma_3$.

**Exercise 2.5.** Prove that $D_8$ is not isomorphic to any symmetric group whatsoever.

**Exercise 2.6.** Prove that $D_{24}$ is not isomorphic to $\Sigma_4$. (Hint: these two groups both have the same order, and they are both non-abelian. You have to think about what properties will distinguish finite non-abelian groups of the same order.)