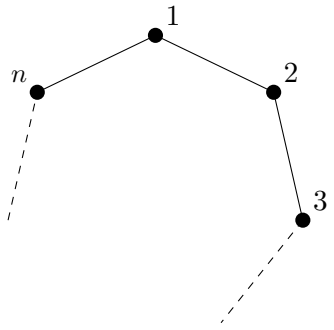
Homework Assignment 3

Due Friday, February 11

1. In class we developed the theory of the group D_{12} of rigid symmetries of the regular hexagon (on bCourses: 'Lecture 4' from 55:00 until the end). In fact, everything we developed should go through almost exactly the same way for D_{2n}: the rigid symmetries of regular n-sided polygon, pictured below:



(a) Explain why D_{2n} is a group under composition of symmetries.

Proof. The definition of symmetry is rather qualitative in nature, so an explanation in plain language here suffices. Essentially by definition, the composition of rigid symmetries is again a rigid symmetry. Also: 'doing nothing' is a rigid symmetry. By definition, a symmetry is reversable implying that inverses exist. Associativity is most easily seen by observing that a symmetry is a type of function from the n-gon to itself. As composition of functions is associative, we win. □

(b) Show that there are exactly $2n$ rigid symmetries of the regular n-gon.

Proof. Fix a symmetry α. We say $\alpha(i) = j$ if the vertex labelled i goes to the point j under the symmetry. Notice that a symmetry can take the vertex labelled 1, to any of the vertices $1, 2, \cdots, n$. This is n choices. So let's make such a choice say $\alpha(1) = i$. Now, we are not allowed to break the n-gon, so that in particular the vertex labeled 2 must end up next to the vertex labeled 1. In particular, $\alpha(2) = i - 1$ or $\alpha(2) = i + 1$ (where we replace the number with the residue mod n where necessary, i.e., if $i = n$ or $i = 1$.) This is 2 choices. Now observe that once these two choices are made, the rest of the symmetry is fixed by rigidity. Indeed, if $\alpha(1) = i$ and $\alpha(2) = i+1$, then $\alpha(3) = i+2$ and $\alpha(4) = i + 3$ and so on. On the other hand, if $\alpha(1) = i$ and $\alpha(2) = i - 1$, then $\alpha(3) = i - 2$ and so on. In each case, we can freely choose from n choices for vertex 1, and then 2 choices for vertex 2, before the symmetry becomes completely determined. This gives precisely $2n$ symmetries. □

(c) Let r be the rotation by $2\pi/n$ in the clockwise direction, and s be the reflection along the vertical line going through the vertex labelled '1'. Compute the elements of D_{2n} in terms of r and s in the following steps:

i. Compute the order of r and s (justifying your answers).

Proof. Notice that r^n is rotation by $\frac{2\pi}{n}n = 2\pi$ so it is the identity function. Suppose $0 < i < n$. Then r^i takes 1 to the $i+1$'st position so that r^i is not the identity. Thus $|r| = n$. For s notice that reflection undoes itseslf, so that s^2 is the identity. But, for example, $s(2) = n$, so that s is not the identity. Therefore $|s| = 2$. □

ii. Let $i_1, i_2 \in \{0, 1\}$ and $j_1, j_2 \in \{0, 1, \cdots, n-1\}$. Show that:

$$s^{i_1}r^{j_1} = s^{i_2}r^{j_2} \text{ if and only if } i_1 = i_2 \text{ and } j_1 = j_2.$$

(Hint: You could first show $s \neq r^i$ for any i using geometry. The rest of the cases should follow from this and part (i) by using cancellation and 8(b).)

Proof. We follow the hint and first show that $s \neq r^i$ for any i. To see this, we first use 8(c) to reduce i modulo n without changing r^i, so that we may freely assume that $i = 0, 1, \cdots, n-1$. Suppose $s = r^i$. Notice that $s(1) = 1$. Since $r^i(1) = i + 1$, we deduce that $i = 0$ as well. But this means r^i is the identity, and s is not the identity, which is a contradiction.

From this we may immediatly deduce that $sr^i \neq r^j$ for any i, j. If not $s = r^{j-i}$, contradicting the previous paragraph.

Lastly, assume $sr^i = sr^j$. Then by cancellation $r^i = r^j$. By HW2 Problem 8(c) we see that $i \equiv j \mod n$ so that $i = j$ since they are both between 0 and $n-1$. □

iii. Conclude that $D_{2n} = \{s^i r^j | i = 0, 1 \text{ and } j = 0, 1, \cdots, n-1\}$. In particular, r and s generate D_{2n}.

Proof. We saw in (c)(ii) that each $s^i r^j$ in the given set is distinct, thus enumerating $2n$ distinct elements of D_{2n}. But by part (b), there are exactly $2n$ elements of D_{2n}, so this must be all of them. □

(d) Show that $rs = sr^{-1}$. Deduce inductively from this that $r^n s = sr^{-n}$ for all n.

Proof. As in part (b), it suffices to show that rs and sr^{-1} agree on 1 and 2. One can observe geometrically that $r(i) = i + 1$ (appropriately reduced mod n), and that s fixes 1 and swaps n and 2. Then we observe:

$$r(s(1)) = r(1) = 2 \qquad s(r^{-1}(1)) = s(n) = 2$$
$$r(s(2)) = r(n) = 1 \qquad s(r^{-1}(2)) = s(1) = 1,$$

This serves as the base case for our induction. For the general case we may assume that $r^{n-1}s = sr^{1-n}$. Then we compute:

$$r^n s = rr^{n-1}s = rsr^{1-n} = sr^{-1}r^{1-n} = sr^{-n},$$

as desired. □

We now completely understand the algebraic structure of D_{2n}. In particular, we know what every element looks like (in terms of r and s) by (c), and we know how to multiply any two elements using the relation in part (d). We summarize this by saying that D_{2n} has the following presentation:

$$D_{2n} = \langle r, s | r^n = s^2 = 1, rs = sr^{-1} \rangle.$$

(e) Use this presentation to give an algebraic proof that every element which is not a power of r has order 2.

Proof. By (c)(iii), the elements which are not powers of r are all sr^i for some i, for the same reason they are nonzero. Then we may compute:

$$(sr^i)^2 = (sr^i)(sr^i) = s(r^i s)r^i = s(sr^{-i})(r^i) = (s^2)(r^{-i}r^i) = 1.$$

□

2. The set S_3 has 6 elements. Compute the order and cycle decomposition of each element.

Proof.
- The identity permutation (1) which has order 1.
- The permutation swapping 1 and 2 and fixing 3. This is (1 2) and has order 2.
- The permutation swapping 1 and 3 and fixing 2. This is (1 3) and has order 2.
- the permutation swapping 2 and 3 and fixing 1. This is (2 3) and has order 2.
- The permutation sending 1 to 2, 2 to 3, and 3 to 1. This is (1 2 3) and has order 3.
- The permutation sending 1 to 3, 3 to 2, and 2 to 1. This is (1 3 2) and has order 3.

□

3. Some of the arguments in problem 1 used a connection between symmetries of polygons and permutations of the vertices. Let's make this explicit!

(a) Describe an injective homomorphism from $\varphi : D_{2n} \to S_n$ (you may describe this in words, but make sure to justify injectivity).

Proof. Label the vertices of the n-gon $\{1, 2, \cdots, n\}$. Then applying a symmetry α give a permutation σ_α of these vertices, thus an element of S_n. This is a well defined function, and it is a homomorphism because composing two symmetries will compose the permutations of the vertices, and multiplication on both sides is exactly composition of functions.

To observe injectivity we leverage 2(c). In particular, we notice that a symmetry is in the kernel precisely when it fixes all the vertices. But only the trivial symmetry does this, so the kernel of φ is trivial. □

(b) In the map you described, what is the cycle decomposition of $\varphi(r)$ (where as usual r is the generator corresponding to clockwise rotation of the n-gon by $2\pi/n$)?

Proof. Consider the rotation r. What permutation does it induce? Well, it sends 1 to 2, 2 to 3, 3 to 4, $\cdots$, $n-1$ to n, and n to 1. But this is precisely the n-cycle (1 2 3 $\cdots$ $n-1$ n). □

(c) Prove that $D_6 \cong S_3$.

Proof. We have described an injective homomorphism $D_6 \to S_3$. But both D_6 and S_3 have 6 elements, so that by HW1 Problem 5 it must be bijective. □

4. No we important basic facts about group homomorphisms that we will use repeatedly throughout the course. Let G, H, K be groups, and let $\varphi : G \to H$ and $\psi : H \to K$ a homomorphisms.

   (a) Show that $\varphi(1_G) = 1_H$.

   Proof. Fix $g \in G$ and let $h = \varphi(g)$. Notice that:

   $$\varphi(1_G) \cdot h = \varphi(1_G)\varphi(g) = \varphi(1_G \cdot g) = \varphi(g) = h.$$

   Mutliplying both sides on the right by h^{-1} we get $\varphi(1_G) = 1_H$ as desired. □

   (b) Show that $\varphi(x^{-1}) = \varphi(x)^{-1}$ for all $x \in G$.

   Proof. Notice that

   $$\varphi(x^{-1})\varphi(x) = \varphi(x^{-1}x) = \varphi(1_G) = 1_H.$$

   Therefore by HW2 7(a) we are done. □

   (c) Show that if $g \in G$ has finite order, then $|\varphi(g)|$ divides $|g|$.

   Proof. Let $m = |g|$ and $n = |\varphi(g)|$. Then

   $$\varphi(g)^m = \varphi(g^m) = \varphi(1_G) = 1_H.$$

   Applying HW2 8(c), we are done. (Explicitly, that problem shows that $m \equiv n \mod n$, which means $n|m$ as desired.) □

   (d) Show that if φ is an isomorphism, then so is φ^{-1}.

   Proof. We already know that φ^{-1} is bijective since it is the inverse to a bijection. Therefore we must show that φ^{-1} is a homomorphism. Fix $x, y \in H$. Then $x = \varphi(a)$ and $y = \varphi(b)$ as φ is bijective. Therefore:

   $$\varphi^{-1}(xy) = \varphi^{-1}(\varphi(a)\varphi(b)) = \varphi^{-1}(\varphi(ab)) = ab = \varphi^{-1}(x)\varphi^{-1}(y).$$

   Therefore φ^{-1} is a homomorphism. □

   (e) Show that if φ is an isomorphism, $|\varphi(g)| = |g|$.

   Proof. There are two cases. First assume $|g| = \infty$. If $\varphi(g)^n = 1$ then

   $$1 = \varphi^{-1}(1) = \varphi^{-1}(\varphi(g)^n) = \varphi^{-1}(\varphi(g^n)) = g^n,$$

   a contradiction as g has infinite order. So therefore $|\varphi(g)| = \infty$ also.
   Otherwise $|g| = n < \infty$. Then $|\varphi(g)| = m$ and $m|n$ by part (c). But by part (d) we can apply part (c) to φ^{-1} and see also that $n|m$. Therefore $n = m$. □

   (f) Show that the composition $\psi \circ \varphi : G \to K$ is a homomorphism.

   Proof. Let $x, y \in G$. Using that ψ and φ are homomorphisms we directly compute:

   $$\psi(\varphi(xy)) = \psi(\varphi(x)\varphi(y)) = \psi(\varphi(x))\psi(\varphi(y))$$

   as desired. □

(g) Suppose φ and ψ are both isomorphisms. Show that the composition $\psi \circ \varphi$ is as well.

Proof. We know the composition is a homomorphism by part (f). Furthermore, the composition of bijective functions is bijective (as in HW2 5), so we win. □

(h) Conclude that the relation *is isomorphic to* is an equivalence relation on the set of all groups.

Proof. Notice that $id_G : G \to G$ is a bijective homomorphism, so that $G \cong G$, proving reflexivity. If $G \cong H$, then there is an isomorphism $\varphi : G \to H$. By part (d) φ^{-1} is an isomorphism too so $H \cong G$ proving symmetry. Finally, if $\varphi : G \cong H$ and $\psi : H \cong K$, then by part (g) $\psi \circ \phi : G \cong K$, proving transitivity. □

5. In this exercise we show that you can compute the order of a permutation from its cycle decomposition.

(a) Let G be a group. Two elements $x, y \in G$ are called *commuting elements* if $xy = yx$. Show that if x and y are commuting elements, then $(xy)^n = x^n y^n$.

Proof. We first show the following identity. If x, y commute, then $x^n y = yx^n$. We proceed by induction on n. If $n = 1$, it is trivial. Now suppose the identity holds for n, we show it does for $n + 1$. Indeed:

$$x^{n+1}y = x^n xy = x^n yx = yx^n x = yx^{n+1}.$$

We now prove the main result. Again we proceed by induction. For $n = 1$ it is trivial. Suppose the identity holds for n. We show it does for $n+1$. Indeed, applying the above identity we see:

$$(xy)^{n+1} = (xy^n)xy = x^n y^n xy = x^n xy^n y = x^{n+1}y^{n+1}.$$

□

(b) Give a counterexample to part (a) if the chosen elements do not commute.

Proof. These are plentiful. We will consider $r, s \in D_{2n}$ for $n \geq 3$. Then $(sr)^2 = 1$ by 1(e). But $s^2 r^2 = r^2 \neq 1$. □

(c) Let $\sigma = (a_1, a_2, \cdots, a_r) \in S_n$ be an r-cycle. Show that $|\sigma| = r$.

Proof. We first show that $|\sigma| \geq r$. Indeed, let $1 \leq k < r$. Then $\sigma^k(a_1) = a_k$ so that σ^k cannot be the identity. It therefore suffices to show that $\sigma^r = 1$. Fix some $b \in \{1, \cdots, n\}$. If $b \neq a_k$ then certainly $\sigma^r(b) = b$ (indeed, $\sigma(b) = b$). Otherwise, $b = a_k$ for some k. Since:

$$(a_1, a_2, \cdots, a_r) = (a_k, a_{k+1}, \cdots, a_r, a_1, a_2, \cdots, a_{k-2}, a_{k-1}),$$

we may assume by relabelling that $k = 1$. But then certainly $\sigma^r(a_1) = a_1$. □

(d) Prove that the order of a permutation is the least common multiple of the lengths of the cycles in its cycle decomposition. (Hint: You may freely use that disjoint cycles are commuting elements. You may find it useful to establish that the product of nontrivial disjoint cycles is never 1).

Proof. We first establish the fact suggested in the hint. Suppose we consider the product of disjoint nontrivial cycles:

$$\sigma = (a_1, \cdots, a_{n_a})(b_1, \cdots, b_{n_b}) \cdots (z_1, \cdots, z_{n_z}).$$

Since theye are disjoint and nontrivial, we see that $\sigma(a_1) = a_2$ so that σ is not the identity.

Now suppose $\sigma = \sigma_1\sigma_2 \cdots \sigma_r$ the cycle decomposition, and the length of each $\sigma_i = \ell_i$. Let m be the least common multiple of the ℓ_i. Then (for example by HW2 8(c)), we knoow that $\sigma_i^m = 1$ for all i, so that applying part (a) we conclude that $\sigma^m = 1$. Therefore $|\sigma| \leq m$. To conlcude, suppose $n < m$. Then there is some i such that $\ell_i \not| n$ (since m is the least common multiple and n is smaller). Again by HW2 8(c), this implies that $\sigma_i^n \neq 1$. So:

$$\sigma^n = \sigma_1^n\sigma_2^n \cdots \sigma_r^n,$$

is the product of disjoint cycles, at least one of which is nontrivial. Therefore it cannot be 1. (We point out that σ_i^n need not be a single cycle, for example, $(1,2,3,4)^2 = (1,3)(2,4)$, but the cycles making up σ_i^n will still be disjoint from those making up σ_j^n). □

6. We suggested in class that if A and B are sets of the same cardinality, then their permutation groups S_A and S_B (defined in HW2#5) are isomorphic. Let's prove it. To begin, fix a bijective function $\theta : A \to B$.

(a) Let $f : A \to A$ be bijective. Show that $\theta \circ f \circ \theta^{-1} : B \to B$ is bijective. (Hint: what is its inverse?)

Proof. As in HW2 5 we know that the composition of bijective functions is bijective. Since θ, f, θ^{-1} are all bijective, so is their composition. □

(b) Part (a) allows us to construct the following function:

$$\begin{array}{ccc} S_A & \xrightarrow{\varphi} & S_B \\ f & \longmapsto & \theta \circ f \circ \theta^{-1}. \end{array}$$

Show that φ is an isomorphism, thereby proving the result. (Note: There are two parts to this. You must show that φ is bijctive, and that it is a homomorphism.)

Proof. We first show that φ is bijective. Indeed, given a permutation $g : B \to B$, we obseve that $\theta^{-1} \circ g \circ \theta : A \to A$ is bijective as in part (a). Therefore $\psi : g \mapsto \theta^{-1} \circ g \circ \theta$ is a function from S_B to S_A. To see it is an inverse to φ we check that:

$$(\psi \circ \varphi)(f) = \psi(\theta \circ f \circ \theta^{-1}) = \theta^{-1} \circ (\theta \circ f \circ \theta^{-1}) \circ \theta = f,$$

and similarly we can see that $(\varphi \circ \psi)(g) = g$. To conclude we must observe that φ is a homomorphism. Let $f, f' \in S_A$. Then:

$$\varphi(f) \circ \varphi(f') = (\theta \circ f \circ \theta^{-1}) \circ (\theta \circ f' \circ \theta^{-1}) = \theta \circ (f \circ f') \circ \theta^{-1} = \varphi(f \circ f'),$$

as desired. □

(c) Use (a) and (b) to conclude that if A be a finite set with n elements, then $S_A \cong S_n$.

Proof. If $|A| = n$ then we can find a bijection between A and the set $[n] = \{1, 2, \cdots, n\}$. (For example, listing $A = \{a_1, a_2, \cdots, a_n\}$ then the bijection $[n] \to A$ could be $i \mapsto a_i$). Therefore, part (c) implies that $S_A \cong S_{[n]}$, but the latter is precisely S_n. □