1 Dihedral groups

Definition 1. D_n (Also written D_{2n}) is the dihedral group on the regular $n-$gon consisting of rotations of the $n-$gon by $\frac{2\pi r}{n}$ for $0 \leq r < n \in \mathbb{Z}$ and reflections over axes of symmetries.

D_n is sometimes also written D_{2n} since D_n has $2n$ elements. The convention is to write σ as rotations and τ as reflections. It is useful to observe that $D_n \leq S_n$ for $n \geq 3$. This tells us that we can think of $\sigma, \tau \in D_n$ as just permutations. By observing the geometry of the $n-$gon alone, we know the following:

Theorem 1. Let σ be a rotation and τ be a reflection. Then, $\tau\sigma = \sigma^{-1}\tau$. For every reflection τ, $\tau^2 = e$. Let τ be a reflection and ρ be rotation by $\frac{2\pi}{n}$. Then, $D_n = \langle \rho, \tau \rangle$. $\langle \rho \rangle$ is a subgroup of order n in D_n.

Geometrically, what is different from rotations and reflections? Let us just ignore the identity rotation for now. Then, one observation that could be made is that rotations never fix an axis, whereas reflections will fix an axis of symmetry. Also, rotations fix an orientation in the sense that if you rotate a point x with a, b as its left and right points respectively, after the rotation, a, b will still be the left and right points of a, but for reflections, there will always be at least one point where this fails.

2 Homomorphisms

Homomorphisms are just a way for you to treat multiplication in one group to be the same as another. You can think of them as analogous to linear transformations in linear algebra. (In fact, they are group homomorphisms under addition)

Definition 2. Let G, H be groups. Then, $\varphi : G \mapsto H$ is called a homomorphism if for all $x, y \in G$, $\varphi(xy) = \varphi(x)\varphi(y)$.

Proposition 1. $\varphi(e) = e$, $\varphi(g^{-1}) = \varphi(g)^{-1}$

Proof. $\varphi(e) = \varphi(e \cdot e) = \varphi(e)\varphi(e)$ so taking the inverse of $\varphi(e)$ to both sides gives $e = \varphi(e)$. $e = \varphi(e) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$ so $\varphi(g)^{-1} = \varphi(g^{-1})$. □

Under homomorphisms, we can define something called the image of φ and the kernel of φ. You can think of them as being analogous to the column space and null space of a linear transformation in linear algebra.

Definition 3. The image of φ is $\text{Im}(\varphi) = \{\varphi(g) | g \in G\}$. The kernel of φ is $\text{Ker}(\varphi) = \{g \in G | \varphi(g) = e\}$.

Proposition 2. The image and kernel of a homomorphism are subgroups of H and G respectively.

Proof. For the image, let $a, b \in \text{Im}(\varphi)$. Then, $ab^{-1} = \varphi(g)\varphi(h)^{-1} = \varphi(g)\varphi(h^{-1}) = \varphi(gh^{-1})$ for some $g, h \in G$ so $\text{Im}(\varphi)$ is a subgroup by the subgroup test. For the kernel, let $a, b \in \text{Ker}(\varphi)$. Then, $\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} = e$ so $\text{Ker}(\varphi)$ is a subgroup by the subgroup test. □

Theorem 2. Let $\varphi : G \mapsto H$ be a homomorphism. Then, φ is injective if and only if $\text{Ker}(\varphi) = \{e\}$.

Proof. We prove each direction in turn.

- For one direction, assume φ is injective. Then, clearly, $\text{Ker}(\varphi) \neq \{e\}$ as otherwise
- For the other direction, assume $\text{Ker}(\varphi) = \{e\}$ and suppose $\varphi(g) = \varphi(h)$. Then, $\varphi(gh^{-1}) = \varphi(g)\varphi(h)^{-1} = e$ and since $\text{Ker}(\varphi) = \{e\}$, we have that $gh^{-1} = e$ and $g = h$.

This proves the statement. □

3 Cayley's theorem

Cayley's theorem is not necessarily very practical in use, and is more so a cool theoretical fact. It is not actually very hard to prove, and is one of the more elementary examples of group actions which we will learn about later.

Theorem 3 (Cayley's theorem)**.** Let G be a group. Then, G is isomorphic to a subgroup of a (possibly infinite) symmetric group.

Proof. Let $g \in G$, and define $\alpha_g : G \mapsto G$ as $\alpha_g(x) = gx$. This map is bijective with the inverse $\beta_g(x) = g^{-1}x$. Now I claim $\varphi(g) \mapsto \alpha_g$ is an injective homomorphism. For it being a homomorphism, $\varphi(g)\varphi(h)(x) = \alpha_g\alpha_h(x) = \alpha_g(hx) = ghx = \alpha_{gh}(x) = \varphi(gh)(x)$ so φ is a homomorphism. For it being injective, assume $\varphi(g) = e$. Then, $gx = x$ for all $x \in G$, so $g = e$ and thus $\text{Ker}(\varphi) = \{e\}$. Then, $\text{Im}(\varphi) \cong G$ is a subgroup of a symmetric group. □

Note that $\text{Im}(\varphi) \cong G$ whenever φ is injective is a consequence of the isomorphism theorems which we will come back to next time.

4 Exercises

1. Let $n \geq 3$. If we view every $\sigma \in D_n$ (σ can be a reflection or rotation) as a permutation in S_n, which σ are even? Which are odd?
2. Let H be a proper subgroup of D_n for $n \geq 3$. Is H cyclic? Prove or disprove.
3. Show that the set of homomorphisms from groups G, H where H is abelian, called $\text{Hom}(G, H)$, is an abelian group under function composition. Show that $\text{Hom}(G, H)$ is not necessarily a group if we assume H is not abelian.
4. Show that the group of automorphisms on G, i.e. isomorphisms $\varphi : G \mapsto G$, denoted $\text{Aut}(G)$, is a group.
5. - Show that $S_n \leq A_{n+2}$ for all n.
   - Let G be a finite group. Show that G is isomorphic to a subgroup of A_n for some n.