Math 411: Honors Algebra I
Problem Set 7
due: October 30, 2019
Emily Riehl

Exercise 1. Define a presentation for the dihedral group $D_{2n}$ with two generators $r$ and $s$. Then justify the relations you enumerate by arguing that every element of the dihedral group has a unique representation as $r^m s^n$ where $m, n \geq 0$ and are each less than the orders of $r$ and $s$ respectively and then sketch a proof that you can reduce any word in the elements $r$ and $s$ can be reduced to a word of the form $r^m s^n$ by iteratively applying the relations you enumerate.

Proof. Let $r$ be a basic rotation and let $s$ be one of the reflections. Then $r^n = e$ and $s^2 = e$. We can check that $rs$ is again a reflection so $(rs)^2 = e$, so $rs = (rs)^{-1} = sr^{n-1}$. Thus $D_{2n}$ has a presentation

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

Now given any element $\sigma$ of $D_{2n}$ either it defines an orientation-preserving action on the $n$-gon (keeping the vertices ordered clockwise, say) or is an orientation-reversing one. In the first case the element is $r^j$ for some $0 \leq j < n$. In the second case $\sigma \cdot s$ is orientation-preserving so $\sigma \cdot s = r^j$ for some $0 \leq j < n$ and thus $\sigma = r^j s$. There are $2n$ elements of $D_{2n}$ and $2n$ elements in the set $\{r^m s^n \mid m < n, k < 2\}$ so we have found the unique representation for each one. \hfill $\square$

Exercise 2. Let $G$ be a group and let $A$ be a set.

(i) Given a group homomorphism $\rho: G \to \text{Aut}(A)$, define a function of two variables $\alpha: G \times A \to A$, the “action of $G$ on $A$,” so that the diagrams

$$
\begin{array}{ccc}
G \times G \times A & \longrightarrow & G \times A \\
\text{id} \times \alpha & \downarrow & \alpha \\
G \times A & \longrightarrow & A
\end{array}
$$

commute in Set.

(ii) Given a function $\alpha: G \times X \to A$ so that the diagrams displayed above commute, define a function $\rho: G \to \text{End}(A)$ and prove that it (a) lands in the subset $\text{Aut}(A) \subset \text{End}(A)$ and (b) defines a group homomorphism.

Proof. (i) Define $\alpha(g, a) = \rho(g)(a)$, the application of the function $\rho(g)$ to the element $a$. We have

\begin{equation}
\alpha(h, \alpha(g, a)) = \alpha(h, \rho(g)(a)) = \rho(h)(\rho(g)(a)) = \rho(hg)(a) = \alpha(hg, a)
\end{equation}

since $\rho$ is a homomorphism and similarly $\alpha(e, a) = \rho(e)(a) = a$ since $\rho(e)$ is the identity function.

(ii) Now given $\alpha$ define $\rho(g): A \to A$ to be the function $a \mapsto \alpha(g, a)$, which is $\rho(g)(-) = \alpha(g, -)$. We can see that $\rho(g)$ is an automorphism since it has an inverse function: namely $\rho(g^{-1})$. We can see that it defines a group homomorphism because $\rho(h)(\rho(g) = \rho(hg)$ by undoing the calculation (1) above.

\hfill $\square$

Exercise 3.

(i) Use the universal property of $\mathbb{Z}/n\mathbb{Z}$ to argue that to define the action of $\mathbb{Z}/n\mathbb{Z}$ on a set $A$ it is necessary and sufficient to define an automorphism $f: A \to A$ of order $n$, i.e., so that $f^n = \text{id}_A$.

(ii) If $G$ is presented by a set of generators $S$ modulo relations $R$, what data is needed to describe a $G$-action?

Proof. By the universal property of $\mathbb{Z}/n\mathbb{Z}$ to define a homomorphism $\mathbb{Z}/n\mathbb{Z} \to G$ it is necessary and sufficient to find an element $g \in G$ so that $g^n = e$. So to define $\mathbb{Z}/n\mathbb{Z} \to \text{Aut}(A)$ we need find $f \in \text{Aut}(A)$ with order $n$, i.e., so that $f^n = \text{id}_A$.

More generally if $G$ is presented by generators $S$ modulo relations $R$, to define $G \to \text{Aut}(A)$ we must define an automorphism $f_s: A \to A$ for every $s \in S$ so that for every relation the corresponding composites of these automorphisms are equal: eg the relation $ts = sf$ would correspond to the composition condition $f_t \circ f_s = f_s \circ f_t$. More formally, to say

---

1 Problems labelled * are optional (fun!) challenge exercises that will not be graded.

2 In class we defined the relations to be elements that generate the kernel of the canonical homomorphism $\phi: F[r,s] \to D_{2n}$ in the sense that the smallest normal subgroup that contains these elements is $\ker \phi$. But for the purposes of applying relations to reduce words, it might be easiest to present your relations as equations between elements of $F[r,s]$. For instance, if $r$ and $s$ commuted (which in this case they do not), this would be expressed by the relation $rs = sr$, which would say that $rsr^{-1}s^{-1}$ is in the kernel of $\phi$ (which, again, is not the case here).
that $G$ is generated by $s_1, ..., s_k \in G$ modulo relations $r_1, ..., r_n \in F[s_1, ..., s_k]$ means that $G \cong F[s_1, ..., s_k]/\langle r_1, ..., r_n \rangle$, where $\langle r_1, ..., r_n \rangle \subset F[s_1, ..., s_k]$ is the smallest normal subgroup containing these elements. By the universal property of quotient groups to define a homomorphism $F[s_1, ..., s_k]/\langle r_1, ..., r_n \rangle \to \text{Aut}(A)$ is to define a homomorphism $\phi: F[s_1, ..., s_k] \to \text{Aut}(A)$ containing $r_1, ..., r_n$ in its kernel. By the universal property of free groups, this amounts to specifying automorphism $f_{s_1}, ..., f_{s_k}$ of $A$ so that for each word $r_i$, the corresponding composite of the automorphisms is the identity function.

**Exercise 4.** The group $\mathbb{Z}/2$ acts on $\mathbb{C}$ by complex conjugation.

(i) Use Exercise 3 to explain what is meant by the previous sentence.

(ii) Any group action on a set defines a partition of that set into orbits. Describe the resulting partition of the complex plane into orbits.

(iii) An element $z \in \mathbb{C}$ is fixed by the complex conjugation action if its orbit is a singleton. What are the fixed points of this action?

**Proof.** To define an action of $\mathbb{Z}/2$ on $\mathbb{C}$, we need to define $\mathbb{Z}/2 \to \text{Aut}(\mathbb{C})$. By the previous problem, it is enough to define an automorphism $f: \mathbb{C} \to \mathbb{C}$ that squares to the identity, i.e., so that $f \circ f = \text{id}$. Complex conjugation $f(x + iy) = x - iy$ has this property.

Each real number $x + i0$ is fixed by the conjugation action, so $\{x\}$ is its own orbit. The other orbits have order 2 and contain complex conjugate pairs $\{x + iy, x - iy\}$. This also answers question (iii).

**Exercise 5.** A Rubik’s cube is built from 26 little cubes called cubies; the expected 27th cubie at the very center of the cube is missing.

(i) Any group action on a set defines a partition of that set into orbits. Describe the resulting partition of the set of 26 cubies into orbits.

(ii) A cubie is fixed by the Rubik’s cube action if its orbit is a singleton. What are the fixed points of the Rubik’s cube action?

**Proof.** The 12 edges are in one orbit, the eight edges are in another orbit, and each of the center pieces is fixed.

**Exercise 6.** Let $H \subset G$ be a subgroup. Then $G$ acts on the set of left cosets $G/H$ by left multiplication as discussed in class.

(i) What is the orbit of the left coset $H$?

(ii) What is the stabilizer of the left coset $H$?

(iii) What is the orbit of a generic left coset $gH$?

(iv) What is the stabilizer of a generic left coset $gH$?

**Proof.** (i) The action of $G$ on $G/H$ is transitive so the orbit of $H$ is the entire set $G/H$.

(ii) The stabilizer of $H$ under this action is $H \subset G$ because $gH = H$ if $g \in H$.

(iii) The transitivity of the action also says the orbit of $gH$ is the entire set $G/H$.

(iv) The stabilizer of $gH$ is the subgroup $gHg^{-1} \subset H$ (see problem 3 on problem set 8 for more about this subgroup). To see this note $kgH = gH$ if and only if $g^{-1}kg \in H$ so the stabilizer is given by those $k$ so that $k \in gHg^{-1}$. All elements of the form $gkg^{-1}$ stabilize $gH$.

**Exercise 7.** Prove that the free group on 26 generators $a, b, c, ..., z$ modulo pronunciation in English is trivial.

---

1 For the purposes of this problem we will consider the cubies to be unoriented.

2 Alternatively, google “homophonic quotients of free groups.”