Dummit & Foote Ch. 1.2: Dihedral Groups

Scott Donaldson

Jan. 2023

1. (1/23/23)

Compute the order of each of the elements in the following groups:

(a) D_6

- r, r^2: 3
- s, sr, sr^2: 2

(b) D_8

- r: 4
- r^2: 2
- r^3: 4
- s, sr, sr^2, sr^3: 2

(c) D_{10}

- r, r^2, r^3, r^4: 5
- s, sr, sr^2, sr^3, sr^4: 2

2. (1/23/23)

Use the generators and relations of $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$ to show that if x is any element of D_{2n} which is not a power of r, then $rx = xr^{-1}$.

Proof. Let $x \in D_{2n}$ such that $x \neq r^k$ for all $k \in \mathbb{Z}$. Then, since all elements of D_{2n} can be written as a product of generators s and r, we must have $x = sr^k$ for some $k \in \{1, 2, ..., n-1\}$. Therefore:

$$rx = rsr^k = sr^{-1}r^k = sr^{k-1} = sr^k r^{-1} = xr^{-1},$$

as desired. $\qquad\square$

3. (1/25/23)

Use the generators and relations above to show that every element of D_{2n} which is not a power of r has order 2. Deduce that D_{2n} is generated by the two elements s and sr, both of which have order 2.

Proof. Let $sr^k \in D_{2n}$. $(sr^k)(sr^k) = s(r^k s)r^k = s(sr^{-k})r^k = ssr^{-k}r^k = 1 \cdot 1 = 1$. Thus the order of elements of the form sr^k, that is, every element which is not a power of r, has order 2.

To show that D_{2n} is generated by s and sr, let $r^k, sr^k \in D_{2n}$. Now $s \cdot sr = r$, so $(s \cdot sr)^k = r^k$. To obtain sr^k, we simply left-multiply the previous by s: $s(s \cdot sr)^k = sr^k$. Thus every element of D_{2n} can be written as a product of s and sr, and so $\langle s, sr \rangle$ is a generator for D_{2n}. $\qquad\square$

4. (1/25/23)

If $n = 2k$ is even and $n \geq 4$, show that $z = r^k$ is an element of order 2 which commutes with all elements of D_{2n}. Show also that z is the only nonidentity element of D_{2n} which commutes with all elements of D_{2n}.

Proof. Let $n = 2k, n \geq 4$, and let $z = r^k \in D_{2n}$. $z \cdot z = r^k r^k = r^{2k} = r^n = 1$, so z has order 2.

Since $r^k r^k = 1$, it follows that $r^k = r^{-k}$ (equivalently, $z = z^{-1}$). Elements of the form r^m obviously commute with each other, so we only need to show that $z = r^k$ commutes with elements of the form sr^m. Now:

$$r^k sr^m = r^k r^{-m} s = r^{-k} r^{-m} s = r^{-k-m} s = (r^{k+m})^{-1} s =$$
$$sr^{k+m} = sr^{m+k} = sr^m r^k,$$

which shows that $z = r^k$ commutes with elements of the form sr^m.

Finally, to show that z is the only nonidentity element which commutes with all elements, we will consider the possible separate cases of the forms of arbitrary elements of D_{2n}. Let $a, b \in D_{2n}$.

- Let $a = r^m$. From above, a commutes with all elements of the form r^p. Does a commute with elements of the form sr^p? $r^m sr^p = r^m r^{-p} s = r^{m-p} s$. On the other hand, we have $sr^p r^m = sr^{p+m} = r^{-p-m} s$. These two are equal when $m - p = -p - m$, that is, when $m = -m$ (in $\mathbb{Z}/n\mathbb{Z}$). This only occurs when $m = n/2 = k$, and so $z = r^k$ is the only element of the form r^m which commutes with all elements of D_{2n}.

- Let $a = sr^m$. As a counterexample, it suffices to show that there is at least one element of D_{2n} which a does not commute with: r. $sr^m r = sr^{m+1}$, while $rsr^m = rr^{-m} s = r^{1-m} s = sr^{m-1}$. Because $n \geq 4$, there are no values of $m \in \mathbb{Z}/n\mathbb{Z}$ for which $m + 1 = m - 1$. Thus elements of the form sr^m do not commute in D_{2n}.

2

This completes the proof that $z = r^k$ is the only nonidentity element of D_{2n} which commutes with all other elements.

$\square$

5. (1/26/23)

If n is odd and $n \geq 3$, show that the identity is the only element of D_{2n} which commutes with all elements of D_{2n}.

Proof. This proof is nearly identical to that of Exercise 4. above, only with n odd instead of even. The proof that elements of the form sr^m is the same as above. To show that elements of the form r^m do not commute, we again consider $r^m sr^p$ and $sr^p r^m$ and see that we must have $m = -m$ (in $\mathbb{Z}/n\mathbb{Z}$). Adding m to both sides, we must have $2m = 0 \Rightarrow 2m = n$. However, because n is odd, this does not occur, and so there are no nonidentity elements of D_{2n} which commute with all elements of D_{2n}.

$\square$

6. (1/26/23)

Let x, y be elements of order 2 in any group G. Prove that if $t = xy$ then $tx = xt^{-1}$ (so that if $n = |xy| < \infty$ then x, t satisfy the same relations in G as s, r do in D_{2n}).

Proof. Let $x, y \in G, |x| = |y| = 2$ and let $t = xy$. From $x^2 = y^2 = 1$, we have $x = x^{-1}$ and $y = y^{-1}$. Then:

$$t = xy \Rightarrow tx = xyx = x(y^{-1}x^{-1}) = x(xy)^{-1} = xt^{-1},$$

as desired.

If $|xy| = |t| = n < \infty$, then we have $t^n = x^2 = 1, tx = xt^{-1}$. These are the same relations in G for x, t as s, r do in D_{2n}.

$\square$

7. (1/26/23)

Show that $\langle a, b \mid a^2 = b^2 = (ab)^n = 1 \rangle$ gives a presentation for D_{2n} in terms of the two generators $a = s$ and $b = sr$ of order 2 computed in Exercise 3 above.

Proof. First, we will show that the relations for r, s follow from the relations for a, b. Let $a = s$, so $s^2 = 1$. Let $r = ab$, so $r^n = (ab)^n = 1$. The orders of r and s are correct, but it remains to be shown that $sr = r^{-1}s$. Now $r = ab = sb$, so left-multiplying both sides by s, we obtain $sr = b$. Also, $r^{-1}s = (ab)^{-1}a = b^{-1}a^{-1}a = b^{-1} = b$. Thus $sr = r^{-1}s$, and so the relations for r, s can be derived from those for a, b.

Next, we will prove the converse, that the relations for a, b follow from those for r, s. Let $a = s$, so $a^2 = 1$. Let $b = sr$, so (from Exercise 3.) $b^2 = (sr)^2 = 1$.

It remains to be shown that $(ab)^n = 1$. Now $ab = s(sr) = r$, and $r^n = 1$, so $(ab)^n = 1$. Thus the relations for a, b can be derived from those for s, r.

Since each set of relations implies the other, they are identical, and thus present the same group, that is, D_{2n}. $\square$

8. (1/26/23)

Find the order of the cyclic subgroup of D_{2n} generated by r.

Proof. Let R be the cyclic subgroup of D_{2n} generated by r, consisting of the elements $\{1, r, r^2, ..., r^{n-1}\}$. Intuitively it contains n elements (half the order of D_{2n}). If less, then some $r^k, k \in \{0, 1, 2, ..., n-1\}$ is excluded from the subgroup, contra the definition of R. If more, then for some element r^k we must have $k > n$ (or else it would not be a unique element). However, since $r^n = 1$, we would then have $r^k = r^{k-n}r^n = r^{k-n}$. If $k - n$ is still greater than n, we would continue this process until we arrive at a $k - mn \in \{0, 1, 2, ..., n-1\}$. In either case, r^k is not unique. Therefore the order of R is exactly n. $\square$

9. (2/2/23)

Let G be the group of rigid motions in $\mathbb{R}^3$ of a tetrahedron. Show that $|G| = 12$.

Proof. Label the vertices of the tetrahedron 1, 2, 3, 4. It has six edges, each labeled by its vertices: 1-2, 1-3, 1-4, 2-3, 2-4, 3-4. A rigid motion maps one edge to another, in either orientation – that is, a rotation in $\mathbb{R}^3$ could map 1-2 to 2-3, the identity would map 1-2 to itself, and a reflection might map 1-2 to 2-1 (swapping the positions of vertices 2 and 1).

If we consider that a motion might send one edge to six possible edges, each with two possible orientations (reflected or not), then there must be 12 unique rigid motions in $\mathbb{R}^3$ of a tetrahedron. $\square$

10. (2/2/23)

Let G be the group of rigid motions in $\mathbb{R}^3$ of a cube. Show that $|G| = 24$.

Proof. Following the pattern of the proof in Exercise 9., there are twelve edges on a cube (labeled by pairs of eight vertices). So a motion might send one edge to twelve possible edges, each with two possible orientations. Thus there are 24 unique rigid motions in $\mathbb{R}^3$ of a cube. $\square$

11. (2/2/23)

Let G be the group of rigid motions in $\mathbb{R}^3$ of an octahedron. Show that $|G| = 24$.

Proof. Like the cube, the octahedron has twelve edges, and therefore $12 \cdot 2 = 24$ unique rigid motions. $\square$

12. (2/3/23)

Let G be the group of rigid motions in $\mathbb{R}^3$ of a dodecahedron. Show that $|G| = 60$.

Proof. The dodecahedron has 30 edges. As with the above proofs, it therefore has 60 rigid motions. $\square$

13. (2/3/23)

Let G be the group of rigid motions in $\mathbb{R}^3$ of an icosahedron. Show that $|G| = 60$.

Proof. The icosahedron has 30 edges. As with the above proofs, it therefore has 60 rigid motions. $\square$

14. (2/3/23)

Find a set of generators for $\mathbb{Z}$.

Proof. $\mathbb{Z}$ is generated by $\langle 1, -1 \rangle$. Every element $n \in \mathbb{Z}$ can be written as $\underbrace{1 + \ldots + 1}_{n \text{ times}}$ (if $n > 0$), $\underbrace{(-1) + \ldots + (-1)}_{n \text{ times}}$ (if $n < 0$), or $1 + (-1)$ (for $n = 0$). $\square$