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. □

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}. □

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}.

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

$\square$