Dan Lyness
Matt Watson

5.2.10. Find $\mathrm{Frat}(D_{2n})$ and $\mathrm{Frat}(D_\infty)$.

Proof. Throughout this proof we use the following representations for D_{2n} and D_∞,

$$D_{2n} = \langle r, s \mid r^n = s^2 = (rs)^2 = 1\rangle$$

$$D_\infty = \langle r, s \mid s^2 = (rs)^2 = 1\rangle.$$

We will show that if $n = p_1^{a_1} \cdots p_k^{a_k}$, then

$$\mathrm{Frat}(D_{2n}) = \langle r^{p_1 p_2 \cdots p_k}\rangle \simeq \mathbb{Z}_{n/(p_1 \cdots p_k)}.$$

We will also show that

$$\mathrm{Frat}(D_\infty) = \{1\}.$$

Claim 1: $\langle r\rangle \le D_{2n}$ and $\langle r\rangle \le D_\infty$ are maximal.

Proof of Claim 1. In the finite case, $|\langle r\rangle| = n \Rightarrow [D_{2n} : \langle r\rangle] = 2$. Since $\langle r\rangle$ has prime index in D_{2n}, $\langle r\rangle$ is maximal in D_{2n}.

In the infinite case, let $\langle r\rangle = H$. Then H and sH are the left cosets of H. These cosets are distinct since $s \notin H$. These are all the cosets since for all $x \in D_\infty$, we can write $x = s^b r^a$ for some integers a and $0 \le b \le 1$. Then $xH = s^b r^a H = s^b H$, since $r^a \in H$. If $b = 0$, $xH = H$ and if $b = 1$, $xH = sH$. Therefore, $[D_\infty : H] = 2$. So $\langle r\rangle$ has prime index and is therefore maximal in D_∞. □Claim 1

Claim 2: Let p be prime. Then $\langle r^p, s\rangle \le D_\infty$ is maximal. If $p \mid n$, then $\langle r^p, s\rangle \le D_{2n}$ is maximal.

Proof of Claim 2. Let $H = \langle r^p, s\rangle \le D_\infty$. We will show that $S = \{H, rH, r^2H, \ldots, r^{p-1}H\}$ are the distinct left cosets of H in D_∞. To see that these cosets are distinct, let $0 \le \ell \le k < p$ and note that $r^k H = r^\ell H \Leftrightarrow r^{k-\ell} \in H$. Thus, $0 \le k-\ell < p$ with $r^{k-\ell} \in H$. But $H = \langle r^p, s\rangle$, so H must contain only elements of that can be represented in the form $r^{mp}s^b$ where $m \in \mathbb{Z}$ and $0 \le b \le 1$. Therefore, $k - \ell = 0 \Rightarrow k = \ell \Rightarrow r^k = r^\ell$. Now we show that S contains all of the left cosets of H. Let $x \in D_\infty$. So, $x = r^a s^b$ for $a \in \mathbb{Z}$ and $0 \le b \le 1$. Consider $xH = r^a s^b H = r^a H$, using the fact that $s \in H$. By the division algorithm, there exists $k \in \mathbb{Z}$ and $0 \le m < p$ such that $a = kp + m$. So, $r^a H = r^m r^{kp} H = r^m H$, which is an element of S. Thus, we have that $[D_\infty : H] = |S| = p$, a prime, so H is maximal in D_∞.

Now let $H = \langle r^p, s\rangle \le D_{2n}$. The proof is the same as the infinite case except for one detail. In the infinite case we immediately knew that elements of H were only elements that could be represented in the form $r^{mp}s^b$, $m \in \mathbb{Z}$ and $0 \le b \le 1$ (this used the fact that r had infinite order). In the finite case, if we assume that $p \mid n$, then we get the same result (only products of r raised to integer multiples of p and s can appear in H). Therefore, if $p \mid n$, then $H \le D_{2n}$ is maximal following from the previous paragraph. □Claim 2

Now we can show that $\mathrm{Frat}(D_\infty) = \{1\}$. By Claims 1 and 2,

$$\mathrm{Frat}(D_\infty) \le \left(\bigcap_{p \text{ prime}} \langle r^p, s\rangle\right) \cap \langle r\rangle = \bigcap_{p \text{ prime}} \langle r^p\rangle = \{1\}.$$

To see that the last equality is true, suppose $n \neq 0$ and $r^n \in \bigcap_{p \text{ prime}} \langle r^p \rangle$. Then n must be divisible by every prime p. But this is impossible since there are an infinite number of primes. Clearly we have $\{1\} \leq \text{Frat}(D_\infty)$, so we have shown that $\text{Frat}(D_\infty) = \{1\}$.

In the finite case, let $n = p_1^{a_1} \cdots p_k^{a_k}$ be the unique prime factorization of n. We have the following similar result following from Claims 1 and 2:

$$\text{Frat}(D_{2n}) \leq \left(\bigcap_{p \text{ prime } p|n} \langle r^p, s \rangle \right) \cap \langle r \rangle = \bigcap_{p|n} \langle r^p \rangle = \langle r^{p_1} \rangle \cap \cdots \cap \langle r^{p_k} \rangle$$

$$= \langle r^{\text{lcm}(p_1, \ldots, p_k)} \rangle = \langle r^{p_1 \cdots p_k} \rangle.$$

Thus, $\text{Frat}(D_{2n}) \leq \langle r^{p_1 \cdots p_k} \rangle$. We want to show the reverse containment. We do this by proving the following claim.

Claim 3: Let $n = p_1^{a_1} \cdots p_k^{a_k}$. Then $r^{p_1 \cdots p_k}$ is a nongenerator of D_{2n}.

Proof of Claim 3. Let $X \subset D_{2n}$ so that $\langle r^{p_1 \cdots p_k}, X \rangle = D_{2n}$. We want to show that $\langle X \rangle = D_{2n}$.

First, we will show that $r \in \langle X \rangle$. Note that $r \in \langle r^{p_1 \cdots p_k}, X \rangle$. It follows that $r = (r^{p_1 \cdots p_k})^\ell r^m$ where $\ell, m \in \mathbb{Z}$ and $r^m \in \langle X \rangle$ (we obtain this expression using the equation $rs = sr^{-1}$ to remove any s from the expression and then collect all powers of $r^{p_1 \cdots p_k}$). Therefore, we have that $r = r^{p_1 \cdots p_k \ell + m} \Rightarrow p_1 \cdots p_k \ell + m \equiv 1 \pmod{n}$. We claim that p_i does not divide m for all i. Suppose for a contradiction that p_i divides m. So, $m = p_i t$ for some integer t. Then,

$$p_i (p_1 \cdots \widehat{p_i} \cdots p_k \ell + t) \equiv 1 \pmod{n}.$$

Thus, p_i is a unit mod n. But this is impossible since $p_i \mid n$. So we have a contradiction, therefore p_i does not divide m. Since the p_i are prime, we have that $\gcd(p_1 \cdots p_k, m) = 1 \Rightarrow \gcd(n, m) = 1$. Since $\langle r \rangle$ is a cyclic group of order n and $\gcd(n, m) = 1$, we have that r^m is also a generator of $\langle r \rangle$. Recall $r^m \in \langle X \rangle$. Thus, $\langle r \rangle = \langle r^m \rangle \subset \langle X \rangle \Rightarrow r \in \langle X \rangle$.

Now we will show that $s \in \langle X \rangle$. We can represent the elements of X as $x_i = r^{b_i} s^{c_i}$ where $0 \leq b_i < n$ and $0 \leq c_i \leq 1$. Suppose for all x_i, $c_i = 0$. Then $\langle r^{p_1 \cdots p_k}, X \rangle \subset \langle r \rangle$, which is a proper subgroup of D_{2n}. This contradicts the fact that $\langle r^{p_1 \cdots p_k}, X \rangle = D_{2n}$. So, there must exist some $x \in X$ such that $x = r^b s$. Since $r \in \langle X \rangle \Rightarrow r^{-b} \in \langle X \rangle$ and $x \in X \Rightarrow x \in \langle X \rangle$, we have that $r^{-b} x = r^{-b} r^b s = s \in \langle X \rangle$.

Since r and s generate D_{2n} and $r, s \in \langle X \rangle$, we have shown that $\langle X \rangle = D_{2n}$. Therefore $r^{p_1 \cdots p_k}$ is a nongenerator of D_{2n}. $\square$Claim 3

Since $\text{Frat}(D_{2n})$ is the set of nongenerators of D_{2n}, we have that $r^{p_1 \cdots p_k} \in \text{Frat}(D_{2n})$ by Claim 3. Therefore, $\langle r^{p_1 \cdots p_k} \rangle \leq \text{Frat}(D_{2n})$. Since $\langle r^{p_1 \cdots p_k} \rangle \leq \langle r \rangle$, a cyclic group of order n with $p_1 \cdots p_k$ dividing n, we have that $\langle r^{p_1 \cdots p_k} \rangle$ is cyclic of order $n/(p_1 \cdots p_k)$. Hence, we have shown that

$$\text{Frat}(D_{2n}) = \langle r^{p_1 p_2 \cdots p_k} \rangle \simeq \mathbb{Z}_{n/(p_1 \cdots p_k)}.$$

$\square$