HW 2

1.2

5.

Let $x = s^k r^i$ be an element which commutes with every element of D_{2n} with $k \leq 1, k < n$. We have $s^k s = ss^k = s^{1-k}$ since s has order 2. Since x commutes with s,

$$\begin{aligned} ss^k r^i &= s^k r^i s \\ s^{1-k} r^i &= s^k s r^{-i} \\ &= s^{k+1} r^{-i} \end{aligned}$$

By equating exponents of s (which we can do because the representation is unique), $1 - k = k + 1$ hence $k = 1$. By equating exponents of r, we have $i = -i \pmod n$ hence $2i = 0 \pmod n$ hence $i = 0 \pmod n$ because n is odd. Hence x is the identity.

7.

$s^2 = a^2 = 1$

$r^n = (s^2 r)^n = (ab)^n = 1$

$rsr = s(sr)(sr) = ab^2 = a = s$. Hence $rs = sr^{-1}$

Conversely,

$a^2 = s^2 = 1$

$b^2 = (sr)^2 = srsr = ss = 1$

$(ab)^n = (ssr)^n = r^n = 1$

1.3

10.

This problem needs the convention $a_0 = a_m$ to be true.

Consider the list $[a_1, a_2, \ldots a_m, a_{m+1} = a_1, \ldots]$ formed by repeating copies of $[a_1, a_2, \ldots a_m]$; label the elements $b_1, b_2 \ldots$. For all natural numbers j we have $\sigma(b_j) = b_{j+1}$. Hence $\sigma^i(b_k) = b_{i+k}$. In particular

$\sigma^i(a_k) = b_{i+k}$. Then $b_{i+k} = a_{j'}$ where j' is $i+k$ replaced by its least residue mod m where $k+i > m$ by construction of the b's.

We have $\sigma^m(a_k) = b_{m+k} = a_k$ hence σ^m is the identity permutation. If $p = ord(\sigma) < m$, then $a_1 = \sigma^p(a_1) = a_{p+1}$ where $p+1$ cannot be reduced further, contradicting the fact that the a's are distinct.

11.

By relabelling, this is equivalent to proving it for the m-cycle $\sigma = (0, 1, 2, \dots m-1)$. Consider the sequence $[0, i, 2i, \dots (m-1)i]$ where each element is reduced mod m. Each element of this sequence is generated by applying σ^i to the previous.

First we show that if m and i are coprime, the sequence consists of distinct elements; then the sequence is the cycle decomposition of σ^i. Supposing otherwise, let $ai = bi$ be two distinct elements of the sequence with $0 \le a < b < m$. Then $ai = bi \pmod{m}$ hence $a = b \pmod{m}$ which is a contradiction.

Conversely, if $gcd(m, i) = g > 1$, then let $k = \frac{m}{g} < m$. We have $ki = \frac{mi}{g} = \frac{lcm(m,i)gcd(m,i)}{g} = lcm(m, i)$. In particular $m|ki$ hence $ki = 0 \pmod{m}$. Then the k-th element of the sequence is 0 and the cycle decomposition of σ^i contains a k-cycle.

15.

We first prove exercise 24: if a, b commute then $(ab)^n = a^n b^n$. First we consider $n \ge 0$.

Lemma: b^n and a commute. We prove this by induction on n. The base case $n = 0$ is trivial. Suppose the result holds for n. Then $b^{n+1}a = bb^n a = bab^n = abb^n = ab^{n+1}$.

Next we do induction on n. The base case $n = 0$ is trivial. Suppose the result holds for n. Then $(ab)^{n+1} = (ab)^n(ab) = a^n b^n ab = a^n ab^n b = a^{n+1}b^{n+1}$.

For negative n, let $p = -n$, we need to prove $(ab)^{-p} = a^{-p}b^{-p}$, equivalently $e = a^{-p}b^{-p}(ab)^p$, equivalently $(ab)^p = a^p b^p$ which is true by the positive n case.

Main theorem: Let $x \in S_n$ be a permutation with (disjoint) cycle decomposition $x = c_1 c_2 \dots c_k$. Let $n \ge 0$. Since disjoint cycles commute, $x^n = c_1^n c_2^n \dots c_k^n$ and these cycles are still disjoint. For $n = ord(x)$, each c_i^n must be the identity (if c_j^n is not the identity, let q be some element that c_j^n, does not fix, then x^n will not fix q either), hence $ord(c_i)|ord(x)$. For $n = lcm(ord(c_1), \dots ord(c_k))$, we have each $c_1^n = 1$ hence $x^n = 1$.

17.

Each such permutation can be written as $(a, b)(c, d)$ where a, b, c, d are distinct and $a < c$. This is in a 3-1 bijection with unordered 4-tuples of $[1, n]$ since the tuple $p < q < r < s$ corresponds to the permutations $(p, q)(r, s)$, $(p, r)(q, s)$ and $(p, s)(q, r)$. Hence there are $3 * \binom{n}{4}$ such permutations.

6a.

It suffices to show that each cycle $(a_1, a_2, \dots a_k)$ is generated by 2-cycles. This is true because $(a_1, a_2, \dots a_k) = (a_1, a_2)(a_2, a_3) \dots (a_{k-1}, a_k)$, which we can see by having it operate on an arbitrary a_j from right to left.

The first 2-cycle that does not fix its argument is (a_j, a_{j+1}) which sends it to a_{j+1}. Now the next 2-cycle is (a_{j-1}, a_j) which fixes a_{j+1}; every other 2-cycle also fixes it since the indices are decreasing.

6b.

The identity has 0 inversions and is even.

A transposition has an even number of inversions. Proof: let the transposition be (a, b) with $a < b$. If $[i, j]$ is a pair with $i < j$ and $i < a$, by considering cases on how j compares with a and b, $\sigma(i) < \sigma(j)$. Hence WLOG we can prove that for S_n the permutation $(1, n)$ is even.

Every pair of indices is one of the following 3 disjoint cases:

If $1 < i < j < n$ then $[i, j]$ is not an inversion.

Let $1 < i < n$. Then $[1, i]$ and $[i, n]$ are both inversions, and are both distinct.

Lastly, $[1, n]$ is an inversion.

Since the inversions in case 2 come in pairs, there is an odd number of inversions.