Section 8: Symmetric Groups

The point of this section is to establish some notation used in talking about the symmetric groups $\mathcal{S}_n$ on finite sets $\{1, 2, \ldots, n\}$. Of course, an element f of $\mathcal{S}_n$ is technically a set of ordered pairs

$$\{(1, f(1)),\ (2, f(2)),\ \ldots,\ (n, f(n))\}$$

and could be written as

$$f:\ 1 \mapsto f(1),\ 2 \mapsto f(2),\ \ldots,\ n \mapsto f(n)\ .$$

But another common notation is

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}\ .$$

So the first row is the set 1 through n in the usual order and the second line is the same set but in any order. (So $\mathcal{S}_n$ is related to the set of all permutations of 1 through n, but the composition of functions makes a group out of this set.) Composition of functions is still done right to left:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

while

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

An even simpler, but not unique, way to write down an element of $\mathcal{S}_n$ is its "disjoint cycle decomposition". First, an r-cycle in $\mathcal{S}_n$ is a function that takes one element, say k_1, of $\{1, 2, \ldots, n\}$ to, say, k_2, k_2 to k_3, and so on until k_{r-1} is taken to k_r, which is taken to k_1; and all the other elements of $\{1, 2, \ldots, n\}$ are taken to themselves. We will write such an r-cycle as $(k_1, k_2, k_3, \ldots, k_r)$. Of course, it could also be written as $(k_2, k_3, \ldots, k_r, k_1)$, or as $(k_3, k_4, \ldots, k_r, k_1, k_2)$, etc. One-cycles are just the identity function, so we will just write them as e (or not at all in a composition with other functions), and 2-cycles (k_1, k_2) are sometimes called *transpositions*. It is easy to see that the order of an r-cycle, as an element of $\mathcal{S}_n$, is r.

Second, we need the following idea:

Def: Two elements f, g of $\mathcal{S}_n$ are called *disjoint* if, for every element k of $\{1, 2, \ldots, n\}$, $f(k) \neq k$ implies $g(k) = k$ (and vice versa); i.e., if f moves k, then g does not.

Prop: Disjoint elements of $\mathcal{S}_n$ commute.

Pf: Suppose f, g are disjoint elements of $\mathcal{S}_n$, and consider any k in $\{1, 2, \ldots, n\}$.

- Suppose first that $g(k) \neq k$. Then because g is one-to-one, $g(g(k)) \neq g(k)$, i.e., g moves both k and $g(k)$, so f cannot move either. So

$$(f \circ g)(k) = f(g(k)) = g(k) \qquad \text{while} \qquad (g \circ f)(k) = g(f(k)) = g(k)\ .$$

- Now suppose $g(k) = k$. Then $f(k)$ may either equal k or not. If $f(k) = k$, then

$$(f \circ g)(k) = f(g(k)) = f(k) = k \qquad \text{while} \qquad (g \circ f)(k) = g(f(k)) = g(k) = k\ ;$$

  while if $f(k) \neq k$, then $f(f(k)) \neq f(k)$, so we must have $g(f(k)) = f(k)$, and hence

$$(f \circ g)(k) = f(g(k)) = f(k) \qquad \text{while} \qquad (g \circ f)(k) = g(f(k)) = f(k)\ .$$

Thus we have $(f \circ g)(k) = (g \circ f)(k)$ for all k in $\{1, 2, \ldots, n\}$, so $f \circ g = g \circ f$.//

Now we argue that any element of $\mathcal{S}$ can be written as a product (composition) of disjoint cycles. If we take a sufficiently large example, it will be clear how to do this in general: Take the following element of $\mathcal{S}_{12}$:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 7 & 6 & 5 & 1 & 4 & 12 & 8 & 10 & 9 & 2 & 11 \end{pmatrix}$$

We begin a cycle with 1, which goes to 3, which goes to 6, which goes to 4, which goes to 5, which goes to 1; so the first cycle is $(1, 3, 6, 4, 5)$. That cycle does not include 2, so we begin a new cycle with 2: 2 goes to 7, which goes to 12, which goes to 11, which goes to 2, so the second cycle is $(2, 7, 12, 11)$. Now 3, 4, 5, 6 and 7 have already appeared in cycles, so we begin a third cycle with 8; but 8 goes to itself, and we do not bother to write the 1-cycle (8). Then 9 goes to 10, which goes to 9, so another cycle is the transposition $(9, 10)$. Because 11 and 12 have already appeared in cycles, our "factorization" of f is complete:

$$f = (1, 3, 6, 4, 5)(2, 7, 12, 11)(9, 10)$$

— or as

$$(6, 4, 5, 1, 3)(7, 12, 11, 2)(9, 10) \qquad \text{or} \qquad (11, 2, 7, 12)(10, 9)(3, 6, 4, 5, 1) \qquad \text{or} \qquad \ldots$$

In this way, every element of any $\mathcal{S}_n$ can be written as the product of disjoint cycles. Because the cycles are disjoint, i.e., move different subsets of $\{1, 2, 3, \ldots, n\}$, and (as a result) they commute, the order of an elements of $\mathcal{S}_n$ is the least common multiple of the lengths of the cycles in its disjoint cycle decomposition. So the order of the f we have been considering is $\text{lcm}(5, 4, 2) = 20$. (Writing down the powers of an r-cycle can be interesting. If r is prime, then all its powers are r-cycles. But if $r = st$, say, then its s-th power is a composition of s disjoint t-cycles.)

Finally, we note that every r-cycle can be written as the product of transpositions (which are not disjoint!): It is easily checked that

$$(k_1, k_2, k_3, \ldots, k_{r-1}, k_r) = (k_1, k_r)(k_1, k_{r-1}) \ldots (k_1, k_3)(k_1, k_2) \ .$$

Thus, for example, the f in $\mathbb{Z}_{12}$ from above could be written as

$$\begin{aligned} f &= (1, 3, 6, 4, 5)\,(2, 7, 12, 11)\,(9, 10) \\ &= (1, 5)(1, 4)(1, 6)(1, 3)\,(2, 11)(2, 12)(2, 7)\,(9, 10) \end{aligned}$$

Because there are r ways of writing an r-cycle, the transpositions in this product are not unique: The same f could also be written as

$$\begin{aligned} f &= (11, 2, 7, 12)\,(10, 9)\,(3, 6, 4, 5, 1) \\ &= (11, 12)(11, 7)(11, 2)\,(10, 9)\,(3, 1)(3, 5)(3, 4)(3, 6) \end{aligned}$$

Also, a transposition has order 2, so we can throw in two copies of any transposition side-by-side anywhere in this product without changing the result. Etc., etc.

But there is one thing that remains constant in <u>all</u> the ways of writing a given element of $\mathcal{S}_n$ as a product of transpositions: the parity — oddness or evenness — of the number of transpositions. The proofs of this fact are ugly, with lots of cases; the text's approach is straightforward and works

reasonably well. But I like the following, which argues that every transposition changes the parity of the number of "backward pairs" in a permutation of 1 through n: In a permutation $k_1, k_2, \ldots, k_n$ of 1 through n, we can look at each of the pairs, i.e., the two-element subsets of $\{1, 2, 3, \ldots, n\}$. If in that permutation a given pair is in its natural order, with the smaller first, the pair is called "forward" in that permutation; if the larger of the pair appears first, it is a "backward pair". So for example in the permutation 3,5,1,2,4, the pairs $\{1,2\}$, $\{1,4\}$, $\{2,4\}$, $\{3,4\}$ and $\{3,5\}$ are forward, while $\{1,3\}$, $\{1,5\}$, $\{2,3\}$, $\{2,5\}$ and $\{4,5\}$ are backward. The argument for the theorem will be based on the following arithmetic fact: Suppose we have two permutations, f and g say, of $1, 2, \ldots, n$, and that f has m backward pairs. Further suppose that in going from f to g, we have changed the "direction" of an odd number of pairs, say $2k+1$ of them — some from forward to backward (say there are p of these), and some from backward to forward (say there are q of these). Then we have $p + q = 2k + 1$, and the number of backward pairs in g is $m + p - q$. Now $m + p - q = m + (p + q) - 2q = m + (2k + 1) - 2q = m + 2(k - q) + 1$, which has a different parity from m; so changing the direction of an odd number of pairs changes the parity of the number of backward pairs.

Thm: If an element of $\mathcal{S}_n$ is written in two different ways as a product of transpositions, then the parities of the numbers of transpositions in the two factorizations are the same.

Pf: Suppose that we compose an element

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}$$

of $\mathcal{S}_n$ with the transposition $g = (r, s)$ where $r < s$:

$$\begin{aligned} fg &= \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix} \begin{pmatrix} 1 & 2 & \ldots & r & \ldots & s & \ldots & n \\ 1 & 2 & \ldots & s & \ldots & r & \ldots & n \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & \ldots & r & \ldots & s & \ldots & n \\ f(1) & f(2) & \ldots & f(s) & \ldots & f(r) & \ldots & f(n) \end{pmatrix} \end{aligned}$$

We want to argue that the number of pairs that have changed from forward to backward or vice versa from the second row of f to the second row of fg is odd; so the parity of the number of backward pairs in the second row of f is different from that of the second row of fg. The result then follows, because the identity has an even number (namely 0) of backward pairs, and each time a transposition is added to the composition, the parity of the backward pairs changes: Odd number of transpositions, odd number of backward pairs; even number of transpositions, even number of backward pairs. But the number of backward pairs is a property of the permutation, independent of which transpositions were composed to get it (as the second row of an element of $\mathcal{S}_n$).

So we look at each of the pairs from $\{1, 2, 3, \ldots, n\}$, in the form $\{f(i), f(j)\}$: If neither i nor j is one of r or s, that pair has the same "direction", either backward or forward, in the second rows of f and fg. The pairs $\{f(i), f(r)\}$ where either $i < r$ or $i > s$ don't change direction in going from f to fg. And the same is true of the pairs $\{f(i), f(s)\}$ where either $i < r$ or $i > s$. The pairs $\{f(i), f(r)\}$ and $\{f(i), f(s)\}$ where i is strictly between r and s all change direction from f to fg; and there are an even number of them — to be exact, $2(s - r - 1)$ of them. Finally, the pair $\{f(r), f(s)\}$ changes direction. So the number of backward pairs does change parity from f to fg.//

Cor and Def: The elements of $\mathcal{S}_n$ that can be written as the composition of an even number of transpositions are called *even permutations.* For $n \geq 2$, they are exactly half of the elements of $\mathcal{S}_n$;

the rest are called *odd permutations.* The set $\mathcal{A}_n$ of all even permutations forms a subgroup of $\mathcal{S}_n$, called the *alternating group* of degree n.

Pf of what is not a definition in this statement: For $n \geq 2$, if f is an even permutation, then $(1,2) \circ f$ is an odd permutation, and if g is odd, then $(1,2) \circ g$ is even. So we have inverse functions $\mathcal{A}_n \to (\mathcal{S}_n - \mathcal{A}_n)$ and $(\mathcal{S}_n - \mathcal{A}_n) \to \mathcal{A}_n$, both given by left composition by $(1,2)$; because they are inverses, they are bijections, so the two sets have the same number of elements; so half the elements of $\mathcal{S}_n$ are odd and half are even.

To see that $\mathcal{A}_n$ is a subgroup, we only need to note that the identity function is even (0 is an even number of transpositions), the composite of two even permutations is even (which is clear), and the inverse of an even permutation is even (reverse the transpositions in the composition to get the inverse; for example, the inverse of $(1,2)(1,3)(2,3)$ is $(2,3)(1,3)(1,2)$ — a permutation is even iff its inverse is also).//

Class participation interlude: Order from the disjoint cycle decomposition. Recall that $(1,4,3,2) = (1,2)(1,3)(1,4)$.

Questions:

1. If an r-cycle is factored into a composite of transpositions as shown in class, how many transpositions are there?
2. So an r-cycle is odd [respectively even] if r is ...
3. An r-cycle has the same parity as the integer ... (looking for a formula)
4. A composition of an r_1-cycle and an r_2-cycle has the same parity as the integer ... (looking for a formula)
5. A composition of s cycles, with lengths $r_1, r_2, \ldots, r_s$ respectively, has the same parity as the integer ... (looking for a formula)

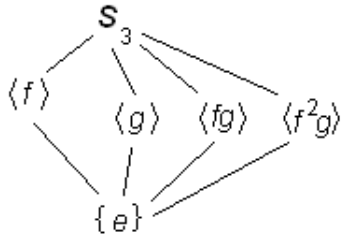
Answers:

1. $r - 1$
2. even [respectively odd]
3. $r - 1$
4. $r_1 + r_2 - 2$
5. $(\sum_{i=1}^{s} r_i) - s$

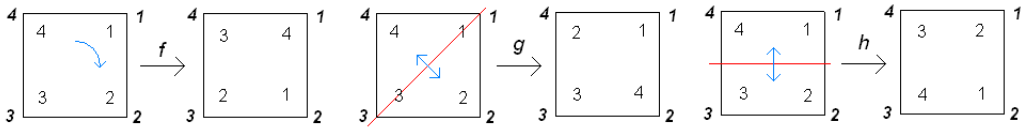
End of interlude

In $\mathcal{S}_3$, where we are using the notation $f = (1,2,3)$ and $g = (1,2)$, we have $\mathcal{A}_3 = \langle f \rangle$, and the odd permutations are g, $fg = (1,3)$ and $f^2 g = (2,3)$. We want to describe the subgroups of $\mathcal{S}_3$: Of course we have $\{e\}$, $\langle f \rangle$ (which has 3 elements), $\langle g \rangle$, $\langle fg \rangle$, $\langle f^2 g \rangle$ (each of which has two elements), and $\mathcal{S}_3$ itself. Now any subgroup that contains both f and g contains all of $\mathcal{S}_3$, so with a little trial and error we can show that there are no other subgroups. (For example, if a subgroup contains both fg and f^2, then it contains $(f^2)^2 = f$ and $f^{-1}(fg) = g$, so it is all of $\mathcal{S}_3$.) The subgroup

lattice is



It was mentioned earlier that the subset of elements of $\mathcal{S}_n$ that preserve some sort of structure often form a subgroup of $\mathcal{S}_n$. One example of this (at least for $n \geq 3$) is the *dihedral group* of degree n, denoted D_n. The idea is that we picture a "regular n-gon", a polygon in the plane that (is not "re-entrant", i.e., it doesn't cross itself, and) has all its sides the same length and all its interior angles the same size, sitting in a frame that fits around it. We consider motions of the regular n-gon that put it back down in the frame, but with n-gon corners in different frame corners. For example, a square, i.e., a regular 4-gon, could be rotated 90° clockwise; or, it could be flipped in its axis of symmetry through two opposite vertices or two opposite sides:



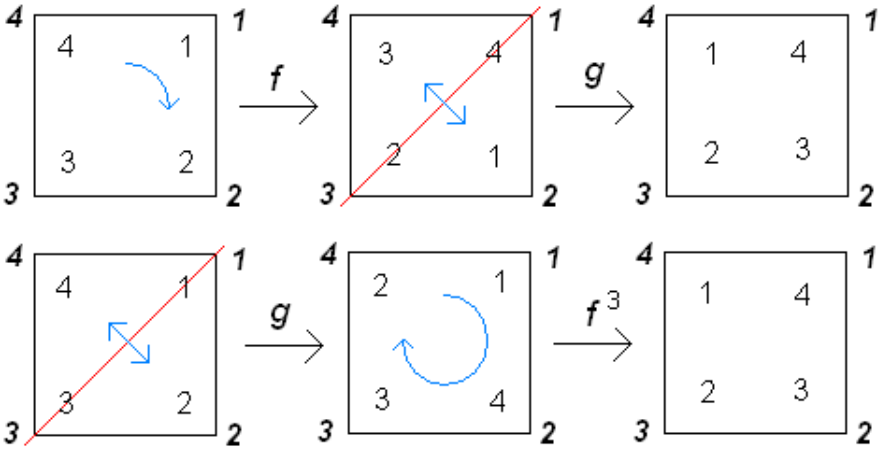
We can make an element of $\mathcal{S}_n$ correspond to such a repositioning as follows: First, we number the vertices of both n-gon and frame in the natural order (let's say clockwise), initially so that the numbers match. Then we reposition the n-gon in the frame. The element of $\mathcal{S}_n$ that corresponds to this motion is given by: the entry in top row gives the number of the n-gon vertex and the entry below it is the number of the frame corner into which it is placed. So the element f of $\mathcal{S}_4$ corresponding to the 90° clockwise rotation is $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1,2,3,4)$, and the one g corresponding to the flip in the 1-3 axis is $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (2,4)$. The set of all elements of $\mathcal{S}_n$ that correspond to such motions of the regular n-gon is denoted D_n. We have n choices for where n-gon corner 1 should go, then only two choices for where corner 2 should go (because it must go to one of the frame corners next to wherever n-gon corner 1 went), and then the rest of the vertices fall into place; so D_n has $2n$ elements. One of these is rotation of $360°/n$, the n-cycle $(1,2,3,\ldots,n)$, and its powers, n of them in all (including the identity). The n-gon has n axes of symmetry (if n is even, half go through two opposite vertices and half through two opposite edges, while if n is odd, they all go through a vertex and the opposite side); flips in these axes of symmetry give n more elements of D_n, each having order 2. But that gives us $2n$ elements of D_n, so we have listed the entire D_n.

In all the various D_n's, we will consistently use the notation f for the rotation $(1,2,\ldots,n)$ through an angle of $360°/n$ clockwise, and g for the flip in the axis of symmetry through the frame vertex labeled 1: $g = (2,n)(3,n-1)\ldots$, where the last ordered pair in g is, if n is even, $(\frac{n}{2}, \frac{n}{2}+2)$ and, if n is odd, $(\frac{n+1}{2}, \frac{n+3}{2})$. We can check that $gf = f^{n-1}g$, either by composing the elements of $\mathcal{S}_n$: [with $n = 4$]

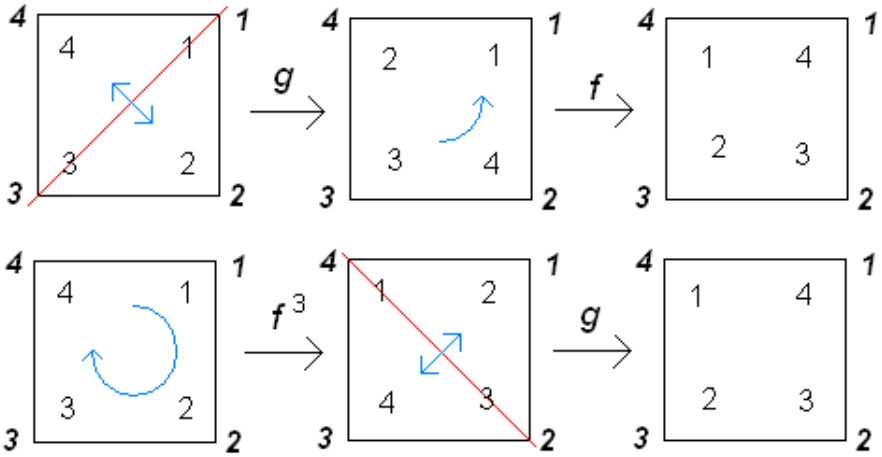
$$gf = (2,4)(1,2,3,4) = (1,4)(2,3)\ , \qquad f^3g = (1,4,3,2)(2,4) = (1,4)(2,3)\ ,$$

or by moving the n-gon in its frame: [again with $n = 4$]

Motions done right to left,
second motion done relative to the frame



Motions done left to right,
second motion done relative to the polygon



(It is natural for readers of English to do things left to right; BUT, because we are thinking of D_n as part of $\mathcal{S}_n$, we should probably always think of doing the motions in D_n from right to left, relative to the frame. So, for example, in D_4, whenever we have g, we should do the flip in the axis from lower left to upper right, no matter where the polygon corner 1 is.) With the equation $gf = f^{n-1}g$ and the fact that $o(f) = n$ and $o(g) = 2$, we can write

$$D_n = \{e, f, f^2, \ldots, f^{n-1}, g, fg, f^2g, \ldots, f^{n-1}g\}$$

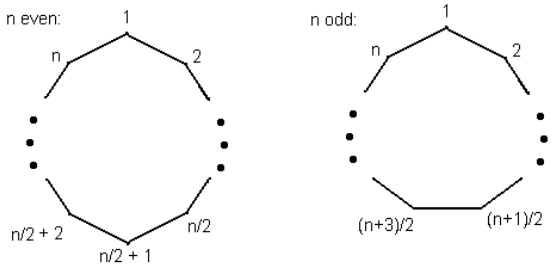
and build the entire group table of D_n. In particular, the f^kg's are the flips in various axes of symmetry and have order 2. You should check that the flip h in the horizontal axis of the square above, $(1,2)(3,4)$ as an element of $\mathcal{S}_n$, is just fg. (Warning: When we turn our attention back to the larger group $\mathcal{S}_n$, or in other groups, we may resume using f and g to mean general elements, not these specific ones. There aren't enough letters available to let some get "bound" for all time to the same meaning.)

Two special cases:

$n = 3$: D_3 is a subgroup of $\mathcal{S}_3$, and $|D_3| = 2(3) = 6 = 3! = |\mathcal{S}_3|$, so they are equal.

$n = 4$: D_4 is a group of 8 elements, having 5 elements of order 2 (the flips and a rotation of 180°), so it is essentially different from the groups $\mathbb{Z}_8$, which has only one; $\mathbb{Z}_2 \times \mathbb{Z}_4$, which has three; $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, which has seven; and the quaternion group Q_8, which has one (and is different from $\mathbb{Z}_8$ because it is nonabelian). So there are at least five different groups of order 8.

Example (just to get used to some of these ideas): What is $\mathcal{A}_n \cap D_n$? Recall that D_n consists of products of f, rotation of the n-gon by one corner inside its frame, and g, flip of the n-gon in its axis of symmetry through vertex 1. Now f, as an element of $\mathcal{S}_n$, is an n-cycle, which is a product of $n-1$ 2-cycles, so it is in $\mathcal{A}_n$ when n is odd. But g is harder: It is the product $(2,n)(3,n-1)\ldots$, where the pairs stop at one of two places, depending on whether n is even or odd:



$$g = \begin{cases} (2,n)(3,n-1)\ldots(n/2,n/2+2) & \text{if} \quad n \text{ is even} \\ (2,n)(3,n-1)\ldots((n+1)/2,(n+3)/2) & \text{if} \quad n \text{ is odd} \end{cases}$$

The number of 2-cycles in g is $n/2-1$ if n is even and $(n+1)/2-1 = (n-1)/2$ if n is odd. So whether g is in $\mathcal{A}_n$ depends on the residue of n mod 4:

- If $n \equiv 0 \mod 4$, then n is even, so $f \notin \mathcal{A}_n$; and the number of 2-cycles in g is $n/2-1$, which is odd, so $g \notin \mathcal{A}_n$. Thus in this case
$$\mathcal{A}_n \cap D_n = \{e, f^2, f^4, \ldots, f^{n-2}, fg, f^3g, \ldots, f^{n-1}g\} \ .$$
- If $n \equiv 1 \mod 4$, then n is odd, so $f \in \mathcal{A}_n$; and the number of 2-cycles in g is $(n-1)/2$, which is even, so $g \in \mathcal{A}_n$. Thus in this case
$$\mathcal{A}_n \cap D_n = D_n \ .$$
- If $n \equiv 2 \mod 4$, then n is even, so $f \notin \mathcal{A}_n$; and the number of 2-cycles in g is $n/2-1$, which is even, so $g \in \mathcal{A}_n$. Thus in this case
$$\mathcal{A}_n \cap D_n = \{e, f^2, f^4, \ldots, f^{n-2}, g, f^2g, \ldots, f^{n-2}g\} \ .$$
- If $n \equiv 3 \mod 4$, then n is odd, so $f \in \mathcal{A}_n$; and the number of 2-cycles in g is $(n-1)/2$, which is odd, so $g \notin \mathcal{A}_n$. Thus in this case
$$\mathcal{A}_n \cap D_n = \{e, f, f^2, \ldots, f^{n-1}\} = \langle f \rangle \ .$$

Please don't try to memorize these cases — this question was only asked to familiarize us with the ideas of $\mathcal{A}_n$ and D_n.

Prop: If H is a subgroup of $\mathcal{S}_n$, then either $H \subseteq \mathcal{A}_n$ or $H \cap \mathcal{A}_n$ consists of half the elements of H.

Pf: Challenge. Hint: If $g \in H$ but $g \notin \mathcal{A}_n$, then $x \mapsto xg$ and $y \mapsto yg^{-1}$ are inverse bijections between $H \cap \mathcal{A}_n$ and $H - (H \cap \mathcal{A}_n)$.//