Dummit & Foote Ch. 1.3: Symmetric Groups

Scott Donaldson

Feb. - Mar. 2023

1. (2/16/23)

- $\sigma : (1, 3, 5)(2, 4)$
- $\tau : (1, 5)(2, 3)$
- $\sigma^2 : (1, 5, 3)$
- $\sigma\tau : (2, 5, 3, 4)$
- $\tau\sigma : (1, 2, 4, 3)$
- $\tau^2\sigma : (1, 3, 5)(2, 4)$ (because $\tau^2 = 1$, so $\tau^2\sigma = \sigma$)

2. (2/16/23)

- $\sigma : (1, 13, 5, 10)(3, 15, 8)(4, 14, 11, 7, 12, 9)$
- $\tau : (1, 14)(2, 9, 15, 13, 4)(3, 10)(5, 12, 7)(8, 11)$
- $\sigma^2 : (1, 5)(3, 8, 15)(4, 11, 12)(7, 9, 4)(10, 13)$
- $\sigma\tau : (1, 11, 3)(2, 4)(5, 9, 8, 7, 10, 15)(13, 14)$
- $\tau\sigma : (1, 4)(2, 9)(3, 13, 12, 15, 11, 5)(8, 10, 14)$
- $\tau^2\sigma : (1, 2, 15, 8, 3, 4, 14, 11, 12, 13, 7, 5, 10)$

3. (2/16/23)

Compute the order of each of the permutations whose cycle decompositions were computed above.

1. $|\sigma| = 6$; $|\tau| = 2$; $|\sigma^2| = 3$; $|\sigma\tau| = 4$; $|\tau\sigma| = 4$; $|\tau^2\sigma| = 6$
2. $|\sigma| = 12$; $|\tau| = 30$; $|\sigma^2| = 6$; $|\sigma\tau| = 6$; $|\tau\sigma| = 6$; $|\tau^2\sigma| = 13$

4. (2/16/23)

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

(a) S_3

- (1): 1
- $(1,2); (1,3); (2,3)$: 2
- $(1,2,3); (1,3,2)$: 3

(b) S_4

- (1): 1
- $(1,2); (1,3); (1,4); (2,3); (2,4); (3,4); (1,2)(3,4);$ $(1,3)(2,4); (1,4)(2,3)$: 2
- $(1,2,3); (1,3,2); (1,2,4); (1,4,2); (1,3,4); (1,4,3);$ $(2,3,4); (2,4,3)$: 3
- $(1,2,3,4); (1,4,2,3); (1,3,2,4); (1,3,4,2); (1,4,2,3); (1,4,3,2)$: 4

5. (2/16/23)

Find the order of $(1,12,8,10,4)(2,13)(5,11,7)(6,9)$.

Proof. The order of a permutation in a symmetric group is the least common multiple of its cycles. However, since we have not yet proven this, we will calculate the first few multiples of the permutation manually, and extrapolate from there. Let $\sigma = (1,12,8,10,4)(2,13)(5,11,7)(6,9)$.

$\sigma^2 = (1,8,4,12,10)(5,7,11)$.

$\sigma^3 = (1,10,12,4,8)(2,13)(6,9)$.

$\sigma^4 = (1,4,10,8,12)(5,11,7)$.

$\sigma^5 = (2,13)(5,7,11)(6,9)$.

From this pattern, we see that each constituent cycle vanishes from the cycle decomposition when the exponent is a multiple of the cycle's length. Thus, the order of σ is the least common multiple of the lengths of its cycles, which is $2 \cdot 3 \cdot 5 = 30$. □

6. (2/17/23)

Write out the cycle decomposition of each element of order 4 in S_4.

- $(1,2,3,4)$
- $(1,2,4,3)$
- $(1,3,2,4)$

- $(1, 3, 4, 2)$
- $(1, 4, 2, 3)$
- $(1, 4, 3, 2)$

7. (2/20/23)

Write out the cycle decomposition of each element of order 2 in S_4.

- $(1, 2)$
- $(1, 3)$
- $(1, 4)$
- $(2, 3)$
- $(2, 4)$
- $(3, 4)$
- $(1, 2)(3, 4)$
- $(1, 3)(2, 4)$
- $(1, 4)(2, 3)$

8. (2/22/23)

Prove that if $\Omega = \{1, 2, 3...\}$ then S_Ω is an infinite group.

Proof. Let $\Omega = \{1, 2, 3...\}$. Consider the subset T consisting of all elements whose cycle decomposition is a single 2-cycle permuting $1 \in \Omega$, for example $(1, 2), (1, 10)$ but not $(2, 3)$.

There is a bijection $f : \mathbb{Z}^+ \to T$ defined by $f(n) = (1, n + 1)$. Because there is a bijection between these two sets, they have the same cardinality; that is, like $\mathbb{Z}^+$, T is infinite.

Because Ω contains a proper subset of infinite size, Ω has infinite elements and is therefore an infinite group.

□

9. (2/22/23)

(a) Let σ be the 12-cycle $(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12)$. For which positive integers i is σ^i also a 12-cycle?

- $\sigma^5 = (1, 6, 11, 4, 9, 2, 7, 12, 5, 10, 3, 8)$
- $\sigma^7 = (1, 8, 3, 10, 5, 12, 7, 2, 9, 4, 11, 6)$
- $\sigma^1 1 = (1, 12, 11, 10, ..., 2)$

(b) Let τ be the 8-cycle $(1, 2, 3, 4, 5, 6, 7, 8)$. For which positive integers i is τ^i also a 12-cycle?

- $\tau^3 = (1, 4, 7, 2, 5, 8, 3, 6)$
- $\tau^5 = (1, 6, 3, 8, 5, 2, 7, 4)$
- $\tau^7 = (1, 8, 7, 6, 5, 4, 3, 2)$

(c) Let ω be the 14-cycle $(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14)$. For which positive integers i is ω^i also a 12-cycle?

- $\omega^3 = (1, 4, 7, 10, 13, 2, 5, 8, 11, 14, 3, 6, 9, 12)$
- $\omega^5 = (1, 6, 11, 2, 7, 12, 3, 8, 13, 4, 9, 14, 5, 10)$
- $\omega^9 = (1, 10, 5, 14, 9, 4, 13, 8, 3, 12, 7, 2, 11, 6)$
- $\omega^{11} = (1, 12, 9, 6, 3, 14, 11, 8, 5, 2, 13, 10, 7, 4)$
- $\omega^{13} = (1, 14, 13, 12, ..., 2)$

10. (2/23/23)

Prove that if σ is the m-cycle $(a_1, a_2, ..., a_m)$, then for all $i \in \{1, 2, 3, ..., m\}$, $\sigma^i(a_k) = a_{k+i}$, where $k+i$ is replaced by its least residue mod m when $k+i > m$. Deduce that $|\sigma| = m$.

Proof. We will prove this by induction on i. For the base case, $i = 1$, we have, by definition, $\sigma^1 = \sigma$ and $\sigma(a_k) = a_{k+1}$ for $k < m$. For m, $\sigma(a_m) = a_1$, and since $1 = (m + 1) \bmod m$, this holds for all $i \in \{1, 2, 3, ..., m\}$.

For the induction case, suppose that for some $n \in \{1, 2, 3, ..., m\}$, $\sigma^n(a_k) = a_{k+n}$ (where $k + n$ is assumed mod m) for all valid k. Consider $\sigma^{n+1} = \sigma^n\sigma^1 = \sigma^n\sigma$. For an arbitrary element a_k, then, $\sigma^{n+1}(a_k) = \sigma^n(\sigma(a_k)) = \sigma^n(a_{k+1})$ (by the base case), which equals a_{k+n+1} (by the induction hypothesis). Therefore, $\sigma^{n+1}(a_k) = a_{k+(n+1)}$.

Thus, by induction, $\sigma^i(a_k) = a_{k+i}$ for all $i \in \{1, 2, 3, ..., m\}$. It follows that $\sigma^m(a_k) = a_{k+m} = a_k$ for all k, so $\sigma^m = 1$. Therefore, $|\sigma| = m$. □

11. (3/12/23)

Let σ be the m-cycle $(1, 2, ..., m)$. Show that σ^i is also an m-cycle if and only if i is relatively prime to m.

Proof. First, we will show that if i and m are relatively prime, then σ^i is also an m-cycle. Let σ be the m-cycle $(1, 2, ..., m)$ and let i be relatively prime to m.

From 10., we know that $\sigma^i(k) = k + i \pmod{m}$. So σ^i is the permutation which sends 1 to $1 + i$, $1 + i$ to $1 + 2i$, and so on. We can represent it with the cycle decomposition $(1, 1 + i, 1 + 2i, ...)$ (all mod m). It may be the case that this includes multiple disjoint cycles – we have not yet proven that σ^i can be represented by a single cycle. However, every element of the first cycle in its cycle decomposition can be represented as $1 + ki$, with $0 \leq k < m$. The final value in the first cycle is $1 + ki$ such that $1 + (k + 1)i = 1$. For this to occur, because i and m are relatively prime, m must divide $k+1$, and so $m \leq k+1$. In fact, we cannot have $m < k + 1$, because when the sequence arrives at $1 + mi$, this is equal to 1. So $m = k + 1$; that is, σ^i is also an m-cycle.

Next, we will prove the contrapositive: Namely, that if i and m are not relatively prime, then σ^i is not an m-cycle. Without loss of generality, let σ be the m-cycle $(1, 2, ..., m)$ and let $j = \gcd\{i, m\} > 1$. Again from 10., $\sigma^i(k) = k+i \pmod{m}$. The first (and possibly only) cycle of the cycle decomposition of σ^i is $(1, 1+i, 1+2i, ...)$ (all mod m). The last element of this cycle decomposition is $1+(\frac{m}{j} - 1)n$. Its successor, $1+\frac{mn}{j}$, is equal to 1 mod m, because m divides $\frac{mn}{j}$. In fact, $\frac{mn}{j}$ is the least common multiple of m and n (because j is the greatest common divisor of m and n). It follows that $\frac{m}{j} - 1$ is the smallest candidate integer for the coefficient of n in the final element of the first cycle. Therefore, σ^i contains a cycle of length $\frac{m}{j} < m$, and so it is not an m-cycle. Further, σ^i contains exactly j disjoint cycles of length $\frac{m}{j}$. □

12. (3/12/23)

(a) If $\tau = (1, 2)(3, 4)(5, 6)(7, 8)(9, 10)$ determine whether there is an n-cycle σ $(n \geq 10)$ with $\tau = \sigma^k$ for some integer k.

Let σ be the 10-cycle $(1, 3, 5, 7, 9, 2, 4, 6, 8, 10)$.

$\sigma^2 = (1, 5, 9, 4, 8)(2, 6, 10, 3, 7)$.

$\sigma^3 = (1, 7, 4, 10, 5, 2, 8, 3, 9, 6)$.

$\sigma^4 = (1, 9, 8, 5, 4)(2, 10, 7, 6, 3)$, and

$\sigma^5 = (1, 2)(3, 4)(5, 6)(7, 8)(9, 10)$.

(b) If $\tau = (1, 2)(3, 4, 5)$ determine whether there is an n-cycle σ $(n \geq 5)$ with $\tau = \sigma^k$ for some integer k.

From 11., we know that if σ is a 5-cycle, then σ^k must be another 5-cycle (because 5 is prime). And, if σ is an n-cycle with $n > 5$, then its cycle decomposition contains disjoint cycles of equal length. Because

$\tau = (1,2)(3,4,5)$ is the product of a 2-cycle and a 3-cycle, there are no n-cycles σ with $n > 5$ and $\tau = \sigma^k$.

13. (3/12/23)

Show that an element has order 2 in S_n if and only if its cycle decomposition is a product of commuting 2-cycles.

Proof. Let $\sigma \in S_n$. First, we will prove that if σ's cycle decomposition is a product of commuting 2-cycles, then σ has order 2. Suppose σ's cycle decomposition can be written $(a_1, a_2)(a_3, a_4)...(a_k, a_{k+1})$ (with k even).

Consider $\sigma^2(a_j)$ for $a_j \in \{a_1, a_2, ..., a_k, a_{k+1}\}$. Generally, $\sigma(a_j) = a_{j+1}$ if j is odd, and a_{j-1} if j is even. Then, if j is odd, $\sigma^2(a_j) = \sigma(\sigma(a_j)) = \sigma(a_{j+1}) = a_j$ (because $j+1$ is even). And, if j is even, $\sigma^2(a_j) = \sigma(\sigma(a_j)) = \sigma(a_{j-1}) = a_j$ (because $j-1$ is odd). σ^2 assigns every $a_j \in \{a_1, a_2, ..., a_k, a_{k+1}\}$ to itself, and every element outside to itself, and is therefore the identity permutation. Thus $|\sigma| = 2$.

Next, let $|\sigma| = 2$, so σ^2 is the identity permutation. Let $(a_1, a_2, ..., a_k)$ be a cycle in σ's cycle decomposition. If $k > 2$, then $\sigma^2(a_1) = \sigma(\sigma(a_1)) = \sigma(a_2) = a_3$. However, this implies that σ^2 is not the identity, a contradiction. Therefore we must have $k \leq 2$. But if $k = 1$, then σ is itself the identity. Thus σ's cycle decomposition is a product of commuting 2-cycles. □

14. (3/12/23)

Let p be prime. Show that an element has order p in S_n if and only if its cycle decomposition is a product of commuting p-cycles. Show by an explicit example that this need not be the case if p is not prime.

Proof. First, to show that if an element in S_n has order p, it is the product of commuting p-cycles, let $\sigma \in S_n$ with $|sigma| = p$. Let $(a_1, a_2, ..., a_k)$ be a cycle in σ's cycle decomposition. From 10., $\sigma^p(a_i) = a_{i+p}$ (with $i + p \bmod k$). Since $\sigma^p = 1$, we must have $i + p \bmod k = i$, so $p \bmod k = 0$. That is, k divides p. Now since p is prime, k must be either 1 or p itself. If $k = 1$, then σ is the identity, which has order 1. Therefore we must have $k = p$. Since an arbitrary cycle of σ is a p-cycle, σ must be a product of commuting p-cycles.

Next, let $\sigma \in S_n$ have a cycle decomposition which is a product of commuting p-cycles. Consider an arbitrary cycle $(a_1, a_2, ..., a_p)$. From 10., this cycle has order p. So every such cycle in σ has order p. Thus σ^p is the product of 1-cycles, and so is the identity permutation. Therefore $|\sigma| = p$. □

15. (3/14/23)

Prove that the order of an element in S_n equals the least common multiple of the lengths of the cycles in its cycle decomposition.

Proof. Consider a permutation $\sigma \in S_n$. σ can be written as the product of commuting cycles. If σ consists of $m > 1$ commuting cycles, then it can be written $\sigma = \sigma_a\sigma_b$, where σ_a consists of $m-1$ commuting cycles and σ_b a single cycle. From 10., σ_b's order is its length.

i) In the case where σ_a and σ_b both are single cycles of length a and b, respectively, then $\sigma_a^a = \sigma_b^b = 1$. Let c be the least common multiple of a and b. Then $\sigma_a^c = 1$ and $\sigma_b^c = 1$, so $(\sigma_a\sigma_b)^c = 1$. Further, c is the smallest positive integer for which $(\sigma_a\sigma_b)^c = 1$, because it is the smallest for which both $\sigma_a^c = 1$ and $\sigma_b^c = 1$. Thus the order of σ is the least common multiple of the length of its cycles.

ii) Now suppose that σ_a is an arbitrary element of S_n with order a, σ_b is a single cycle with order b, and $\sigma_a\sigma_b$ has order c. From Ch. 1, exercise 24., if a and b are commuting group elements, then $(ab)^k = a^k b^k$. Then $(\sigma_a\sigma_b)^c = \sigma_a^c\sigma_b^c$. Since the product has order c, raised to the power of c, it equals 1, so $\sigma_a^c\sigma_b^c = 1$. Because σ_a and σ_b commute, they have disjoint cycle decompositions, and therefore cannot be each other's inverses. Then we must have $\sigma_a^c = 1$ and $\sigma_b^c = 1$. From $|\sigma_a| = a$ and $|\sigma_b| = b$, we know that both a and b divide c. By definition, then, c is the least common multiple of a and b. Thus the order of $\sigma_a\sigma_b$ is the least common multiple of the orders of σ_a and σ_b.

Finally, for any given permutation σ in S_n, to find its order, proceed like this: Take the first two single cycles of σ. As shown above in i), the order of their product is the least common multiple of their lengths. Next take the first three cycles. We now know the order of the product of the first two, and from above in ii), we know that the order of the product of the three is least common multiple of the third's cycle length together with the order of the first two (that is, the least common multiple of their cycle lengths). So the order of first three cycles is the least common multiple of their cycle lengths. One can proceed thusly to show that, for any positive m, the order of the product of the first m cycles is the least common multiple of their cycle lengths. Thus the order of σ is the least common multiple of the cycle lengths of its cycle decomposition. □

16. (3/15/23)

Show that if $n \geq m$ then the number of m-cycles in S_n is given by

$$\frac{n(n-1)(n-2)...(n-m+1)}{m}.$$

Proof. Let $\Omega = \{1, 2, 3, ..., n\}$, let S_n be the symmetric group on Ω, and let $\sigma \in S_n$ be a permutation on elements of Ω with a cycle decomposition that is a single m-cycle with $m \leq n$. To count the ways of forming σ, first consider all m-cycles. There are n choices for the first element, $n-1$ for the second, $n-2$ for the third, and so on, so that there are $n(n-1)(n-2)...(n-m+1)$ ways to form an m-cycle in general.

However, this ignore the fact that many m-cycles represent the same σ, for example $(1, 2, 3) = (2, 3, 1)$. Let $\sigma = (a_1, a_2, ..., a_m)$ be an m-cycle. The cycles $(a_2, a_3, ..., a_m, a_1), (a_3, a_4, ..., a_m, a_1, a_2), ..., (a_m, a_1, ..., a_{m-1})$ all represent the same permutation as σ. That is, there are m possible ways of representing an arbitrary m-cycle, and therefore the number of unique m-cycles in S_n is $n(n-1)(n-2)...(n-m+1)/m$. □