Dummit & Foote Ch. 3.5: Transpositions and the Alternating Group

Scott Donaldson

Dec. 2023

1. (12/6/23)

In Exercises 1 and 2 of Section 1.3 you were asked to find the cycle decompositions of some permutations. Write each of these permutations as a product of transpositions. Determine which of these is an even permutation and which is an odd permutation.

In Exercise 1,

$$\begin{aligned}
\sigma &= (1,3,5)(2,4) = (1,3)(1,5)(2,4),\ \text{odd.}\\
\tau &= (1,5)(2,3),\ \text{even.}\\
\sigma^2 &= (1,5,3) = (1,3)(1,5),\ \text{even.}\\
\sigma\tau &= (2,5,3,4) = (2,4)(2,3)(2,5),\ \text{odd.}\\
\tau^2\sigma &= (1,3,5)(2,4) = (1,5)(1,3)(2,4),\ \text{odd.}
\end{aligned}$$

In Exercise 2,

$$\begin{aligned}
\sigma &= (1,13,5,10)(3,15,8)(4,14,11,7,12,9)\\
&= (1,10)(1,5)(1,13)(3,8)(3,15)(4,9)(4,12)(4,7)(4,11)(4,14),\ \text{even.}\\
\tau &= (1,14)(2,9,15,13,4)(3,10)(5,12,7)(8,11)\\
&= (1,14)(2,4)(2,13)(2,15)(2,9)(3,10)(5,7)(5,12)(8,11),\ \text{odd.}\\
\sigma^2 &= (1,5)(3,8,15)(4,11,12)(7,9,4)(10,13)\\
&= (1,15)(3,15)(3,8)(4,12)(4,11)(7,4)(7,9)(10,13),\ \text{even.}\\
\sigma\tau &= (1,11,3)(2,4)(5,9,8,7,10,15)(13,14)\\
&= (1,3)(1,11)(2,4)(5,15)(5,10)(5,7)(5,8)(5,9)(13,14),\ \text{odd.}\\
\tau\sigma &= (1,4)(2,9)(3,13,12,15,11,5)(8,10,14)\\
&= (1,4)(2,9)(3,5)(3,11)(3,15)(3,12)(3,13)(8,14)(8,10),\ \text{odd.}\\
\tau^2\sigma &= (1,2,15,8,3,4,14,11,12,13,7,5,10)\\
&= (1,10)(1,5)(1,7)(1,13)(1,12)(1,11)(1,14)(1,4)(1,3)(1,8)(1,15)(1,2),\\
&\quad \text{even.}
\end{aligned}$$

2. (12/6/23)

Prove that σ^2 is an even permutation for every permutation σ.

Proof. We take as given the homomorphism $\epsilon : S_n \to \{\pm 1\}$ defined in this chapter, which determines the sign of every permutation $\sigma \in S_n$.

If σ is an even permutation, then $\epsilon(\sigma) = 1$. It follows that:

$$\epsilon(\sigma^2) = \epsilon(\sigma)\epsilon(\sigma) = 1 \cdot 1 = 1,$$

and so σ^2 is an even permutation.

If σ is an odd permutation, then $\epsilon(\sigma) = -1$. It follows that:

$$\epsilon(\sigma^2) = \epsilon(\sigma)\epsilon(\sigma) = -1 \cdot -1 = 1,$$

and so σ^2 is an even permutation.

Since for every $\sigma \in S_n$, σ is either an even or an odd permutation, this proves that σ^2 is an even permutation for every permutation σ. □

3. (12/6/23)

Prove that S_n is generated by $\{(i, i+1) \mid 1 \leq i \leq n-1\}$.

Proof. Since any element of S_n may be written as a product of transpositions, it suffices to show that the set $\{(i, i+1) \mid 1 \leq i \leq n-1\}$ can generate any transposition. Writing an arbitrary transposition in S_n as $(i, i+a)$, we will prove this by strong induction on a (where $1 \leq a \leq n-i$).

The base case $a = 1$ is given, since $(i, i+1)$ is a member of the generating set for all $i \in \{1, ..., n-1\}$.

Next, suppose that for all $i \in \{1, ..., n-1\}$ and $a \in \{1, ..., n-i\}$, the transposition $(i, i+a-1)$ can be obtained from the generating set. So we have the transpositions $(i+a-1, i+a)$ (in the generating set) and $(i, i+a-1)$ (from the inductive hypothesis). Then:

$$(i+a-1, i+a)(i, i+a-1)(i+a-1, i+a) = (i, i+a),$$

so we can obtain the transposition $(i, i+a)$. This concludes the proof that the set $\{(i, i+1) \mid 1 \leq i \leq n-1\}$ can generate any transposition, and therefore generates all of S_n. □

4. (12/7/23)

Show that $S_n = \langle (1, 2), (1, 2, 3, ..., n) \rangle$ for all $n \geq 2$.

Proof. Note that:

$$\begin{aligned}
&(1,2,3,...,n)(1,2)(1,2,3,...,n)^{-1}\\
&=(1,2,3,...,n)(1,2)(1,n,n-1,...,2)\\
&=(2,3),
\end{aligned}$$

and in general,

$$\begin{aligned}
&(1,2,3,...,n)(i,i+1)(1,2,3,...,n)^{-1}\\
&=(1,2,3,...,n)(i,i+1)(1,n,n-1,...,2)\\
&=(i+1,i+2)
\end{aligned}$$

for $1 \leq i \leq n-1$ (if $i = n-1$, then the resulting transposition is equal to $(1, n)$).

This shows that every transposition of adjacent integers can be obtained from $\langle(1,2),(1,2,3,...,n)\rangle$, and from the results of Exercise 3, it therefore generates all of S_n. □

5. (12/7/23)

Show that if p is prime, $S_p = \langle\sigma, \tau\rangle$ where σ is any transposition and τ is any p-cycle.

Proof. Let $\tau = (a_1, a_2, ..., a_p)$ and $\sigma = (a_i, a_{i+k})$, where $1 \leq i < p$ and $i < k \leq p - i$. Note that:

$$\begin{aligned}
\tau\sigma\tau^{-1} &= (a_1,a_2,...,a_p)(a_i,a_{i+k})\\
&\qquad(a_1,a_p,a_{p-1},...,a_2)\\
&=(a_{i+1},a_{i+k+1}),\ \text{and so:}\\
(\tau^2)\sigma(\tau^2)^{-1}=\tau(\tau\sigma\tau^{-1})\tau^{-1} &= (a_1,a_2,...,a_p)(a_{i+1},a_{i+k+1})\\
&\qquad(a_1,a_p,a_{p-1},...,a_2)\\
&=(a_{i+2},a_{i+k+2}),\ \text{and in general:}\\
(\tau^n)\sigma(\tau^n)^{-1}=\tau((\tau^{n-1})\sigma(\tau^{n-1})^{-1})\tau^{-1} &= (a_1,a_2,...,a_p)(a_{i+n-1},a_{i+k+n-1})\\
&\qquad(a_1,a_p,a_{p-1},...,a_2)\\
&=(a_{i+n},a_{i+k+n}),
\end{aligned}$$

where all subscripts are taken mod p if they are greater than p.

Next, we define a set:

$$\begin{aligned}
\Sigma &= \{(\tau^n)\sigma(\tau^n)^{-1} \mid 0 \leq n < p\}\\
&=\{(a_j,a_{j+k}) \mid 1 \leq j \leq p\}.
\end{aligned}$$

Clearly Σ is generated by σ and τ. We claim that Σ generates any transposition of the form (a_j, a_{j+nk}), where $1 \leq j \leq p$, $n \geq 1$. We will show this by strong induction on n.

The base case $n = 1$ is given by the construction of Σ, since it contains all transpositions of the form (a_j, a_{j+k}).

Next, suppose that Σ can generate any transposition of the form (a_j, a_{j+mk}), where $1 \leq m < n$. Then:

$$\underbrace{(a_j, a_{j+(n-1)k})}_{m=n-1}\underbrace{(a_{j+(n-1)k}, a_{j+nk})}_{m=1}\underbrace{(a_j, a_{j+(n-1)k})}_{m=n-1} = (a_j, a_{j+nk}),$$

which shows that we can generate any transposition of the form (a_j, a_{j+nk}).

Now since p is prime, for any transposition (a_j, a_{j+q}), we can write $q = nk \mod p$ for some $n \geq 1$. Therefore Σ can generate any transposition in S_p, and it therefore generates all of S_p. $\square$

6. (12/7/23)

Show that $\langle(1,3),(1,2,3,4)\rangle$ is a proper subgroup of S_4. What is the isomorphism type of this subgroup?

Proof. First, we will define a map $\varphi : D_8 \to \langle(1,3),(1,2,3,4)\rangle$ and show that it is an isomorphism. Since the order of D_8 is strictly less than S_4, we will conclude that $\langle(1,3),(1,2,3,4)\rangle$ is a proper subgroup of S_4.

Define φ such that $\varphi(s) = (1,3)$ and $\varphi(r) = (1,2,3,4)$. We will first show that φ is a homomorphism. The orders of s and r hold under φ, since $s^2 = 1$ and $(1,3)^2 = (1)$, and $r^4 = 1$ and $(1,2,3,4)^4 = (1)$. Also, the relation in D_8 that $sr = r^{-1}s$ holds under φ:

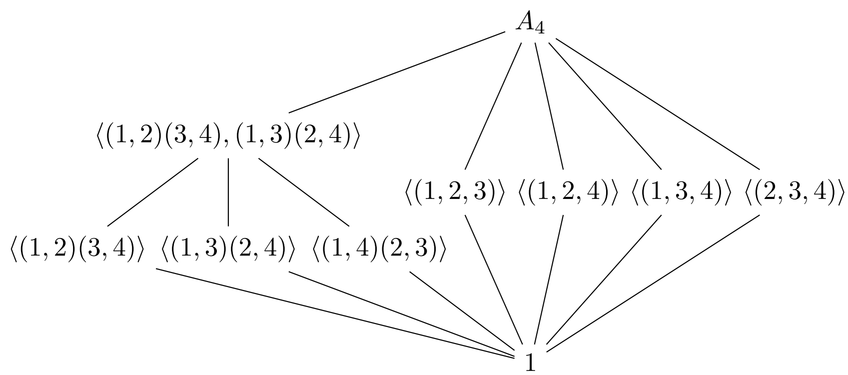
$$\varphi(s)\varphi(r) = (1,3)(1,2,3,4) = (1,2)(3,4) = (1,4,3,2)(1,3) = \varphi(r)^{-1}\varphi(s).$$

Since φ is defined on the generators of D_8 to the generators $(1,3)$ and $(1,2,3,4)$, φ is surjective.

We next show that $\langle(1,3),(1,2,3,4)\rangle$ contains 8 elements. The cyclic group generated by $(1,2,3,4)$ contains 4 elements. Its left and right cosets with $(1,3)$ are equal to each other, so there are therefore no other elements that can be generated. Since $|\langle(1,3),(1,2,3,4)\rangle| = |D_8|$ and there exists a surjective homomorphism between them, φ is necessarily an isomorphism, so $\langle(1,3),(1,2,3,4)\rangle \cong D_8$. We conclude that it is a proper subgroup of S_4. $\square$

8. (12/8/23)

Prove the lattice of subgroups of A_4 given in this text is correct.



Proof. The alternating group A_4 has order $|S_4|/2 = 12$. By Lagrange's Theorem, its proper subgroups must have order 2, 3, 4, or 6.

It contains no subgroups generated by a single transposition, e.g. $\langle (1,2) \rangle$, since these contain odd permutations. The other subgroups generated by an element of order 2 are all shown above.

The lattice also contains all subgroups generated by a single 3-cycle, e.g. $\langle (1,2,3) \rangle$. There might be a proper subgroup of order 6 containing one of these. However, the join of $\langle (1,2,3) \rangle$ with another 3-cycle or with a pair of disjoint transpositions produces all of A_4. Since there are no other permutations in A_4, this implies that there is no proper subgroup containing the cyclic group generated by a 3-cycle.

Finally, the join of two order 2 subgroups produces $\langle (1,2)(3,4),(1,3)(2,4) \rangle$, isomorphic to V_4. Since this subgroup is of index 3 in A_4, there are no other subgroups of A_4, and thus the lattice displayed above is correct and complete. $\square$