Solution for Homework 6

Xiangcan Li

March 22, 2021

Exercise 3.4.1 Let $\tau \in S_n$ and suppose that $\sigma = (k_1\ k_2\ \ldots\ k_j)$ is a j–cycle. Prove that the conjugate of σ by τ is also a j–cycle, and is given by

$$\tau\sigma\tau^{-1} = (\tau(k_1)\ \tau(k_2)\ \ldots\ \tau(k_j)).$$

Further prove that if σ' is any other j–cycle, then σ and σ' are conjugate.

Given $k \geq 2$, a k–cycle in S_n is a permutation σ with the property that $\{1, \ldots, n\}$ is the union of two disjoint subsets, $\{1, \ldots, n\} = Y \cup Z$ and $Y \cap Z = \emptyset$, such that

1. $\sigma(x) = x$ for every $x \in Z$, and
2. $|Y| = k$, and for any $x \in Y$, $Y = \{\sigma(x), \sigma^2(x), \sigma^3(x), \ldots, \sigma^{k-1}(x), \sigma^k(x) = x\}$.

Since σ is a j-cycle, σ cyclically permutes $\{k_1, k_2 \ldots, k_j\}$ and fixes $\{k_{j+1}, \ldots, k_{j+n}\}$, where $\{k_1, k_2 \ldots, k_j\} \cup \{k_{j+1}, \ldots, k_{j+n}\} = S_n$ and $\{k_1, k_2 \ldots, k_j\} \cap \{k_{j+1}, \ldots, k_{j+n}\} = 0$.

Then we have

$$\begin{aligned}
\tau\sigma\tau^{-1}(\tau(k_1)) &= \tau(\sigma(k_1)) = \tau(k_2) && \sigma(k_1) = k_2 \\
\tau\sigma\tau^{-1}(\tau(k_2)) &= \tau(\sigma(k_2)) = \tau(k_3) && \sigma(k_2) = k_3 \\
&\vdots \\
\tau\sigma\tau^{-1}(\tau(k_{j-1})) &= \tau(\sigma(k_{j-1})) = \tau(k_j) && \sigma(k_{j-1}) = k_j \\
\tau\sigma\tau^{-1}(\tau(k_j)) &= \tau(\sigma(k_j)) = \tau(k_1) && \sigma(k_j) = k_1 \\
\tau\sigma\tau^{-1}(\tau(k_1)) &= \tau(\sigma(k_1)) = \tau(k_2) && \sigma(k_1) = k_2
\end{aligned}$$

and $\tau\sigma\tau^{-1}(\tau(k)) = \tau\sigma(k) = \tau(k)$ for $k \in \{k_{j+1}, \ldots, k_{j+n}\}$.

Hence, $\tau\sigma\tau^{-1} = (\tau(k_1)\ \tau(k_2)\ \ldots\ \tau(k_j))$ and $\tau\sigma\tau^{-1}$ is also a j-cycle.

Let $\sigma' = \{l_1\ \ldots\ l_j\}$ is an arbitrary j-cycle different from σ.

Consider $\tau \in S_n$ as $\tau(k_1) = l_1, \ldots, \tau(k_j) = l_j$ and $\tau(k) = f(k)$ for $k \in \{k_{j+1}, \ldots, k_{j+n}\}$, where $f : \{k_{j+1}, \ldots, k_n\} \to \{l_{j+1}, \ldots, l_n\}$ is bijective.

Then we have

$$\begin{aligned}
\tau\sigma\tau^{-1}(l_1) &= \tau\sigma(k_1) = \tau(k_2) = l_2 = \sigma'(l_1) \\
\tau\sigma\tau^{-1}(l_2) &= \tau\sigma(k_2) = \tau(k_3) = l_3 = \sigma'(l_2) \\
&\vdots \\
\tau\sigma\tau^{-1}(l_{j-1}) &= \tau\sigma(k_{j-1}) = \tau(k_j) = l_j = \sigma'(l_{j-1}) \\
\tau\sigma\tau^{-1}(l_j) &= \tau\sigma(k_j) = \tau(k_1) = l_1 = \sigma'(l_j).
\end{aligned}$$

Note that $\tau^{-1}(l) \in \{k_{j+1}, \ldots, k_{j+n}\}$ for $l \in \{l_{j+1}, \ldots, l_n\}$. Then $\sigma(\tau^{-1}(l)) = \tau^{-1}(l)$ for $l \in \{l_{j+1}, \ldots, l_n\}$.

Hence, $\tau\sigma\tau^{-1}(l) = \tau\tau^{-1}(l) = l = \sigma'(l)$ for $l \in \{l_{j+1}, \ldots, l_n\}$.

We conclude $\sigma' = \tau\sigma\tau^{-1}$. Since σ' is arbitrary, if σ' is any other j–cycle, then σ and σ' are conjugate.

Exercise 3.4.2 Suppose $\sigma_1, \sigma_2 \in S_n$. Using the previous exercise, prove that σ_1 and σ_2 have the same cycle structure if and only if they are conjugate.

- $\Longrightarrow$: By proposition 1.3.5, given $\sigma_1, \sigma_2 \in S_n$, there exists a set of pairwise disjoint cycles $\sigma'_1, \ldots, \sigma'_m, \sigma''_1, \ldots, \sigma''_m \in S_n$, so that $\sigma_1 = \sigma'_1 \circ \ldots \circ \sigma'_m$ and $\sigma_2 = \sigma''_1 \circ \ldots \circ \sigma''_m$.

  By Lemma 1.3.4, σ'_i and σ'_j commute. σ''_i and σ''_j also commute. Note that σ_1 and σ_2 have the same cycle structure. We rearrange the order and obtain two new sequences of composition of cycles

  $$\sigma_1 = \sigma'_1 \circ \ldots \circ \sigma'_m \text{ and } \sigma_2 = \sigma''_1 \circ \ldots \circ \sigma''_m,$$

  so that $\{\sigma'_1\} = \{\sigma''_1\}, \ldots, \{\sigma'_m\} = \{\sigma''_m\}$, where $\{\sigma\}$ denotes the length of cycle σ.

  For each σ'_i and σ''_i, we have $\sigma'_i = (k_1 \ \ldots \ k_p)$ and $\sigma''_i = (l_1 \ \ldots \ l_p)$. Consider $\tau_i : \{k_1, \ldots, k_p\} \to \{l_1, \ldots, l_p\}$ be $\tau_i(k_j) = l_j$. Then we get $\tau_1, \ldots, \tau_m$ Define f as $f : \{a_1, \ldots, a_q\} \to \{b_1, \ldots, b_q\}$ such that f is bijective, where σ_1, σ_2 fix $\{a_1, \ldots, a_q\}, \{b_1, \ldots, b_q\}$, respectively. Note that we are able to get a bijective map f since $|S_n| - \{\sigma_1\} = |\{a_1, \ldots, a_q\}| = |\{b_1, \ldots, b_q\}| = |S_n| - \{\sigma_2\}$.

  Let $\tau = \tau_1 \circ \ldots \circ \tau_n \circ f$ and a_i, b_j denote ith and jth element in $\{a_1, \ldots, a_n\}, \{b_1, \ldots, b_n\}$, respectively, such that $\tau(a_i) = b_j$. Let k_{ij}, l_{ij} denote jth element in σ'_i, σ''_i, respectively. Then we have

  $$\tau\sigma_1\tau^{-1}(l_{ij}) = \tau\sigma_1(k_{ij}) = \tau(k_{i(j+1)}) = l_{i(j+1)} = \sigma_2(l_{ij}) \text{ and}$$

  $$\tau\sigma_1\tau^{-1}(b_j) = \tau\sigma_1(a_i) = \tau(a_i) = b_j = \sigma_2(b_j).$$

  Hence, σ_1 and σ_2 are conjugates.

- $\Longleftarrow$: By Exercisse 3.4.1, for some $\tau \in S_n$, we have $\tau\sigma_1\tau^{-1} = \sigma_2$. By proposition 1.3.5, given $\sigma_1 \in S_n$, there exists a set of pairwise disjoint cycles $\sigma'_1, \ldots, \sigma'_m$ such that $\sigma_1 = \sigma'_1 \circ \ldots \circ \sigma'_m$.

  Then we have

  $$\begin{aligned}\sigma_2 &= \tau\sigma_1\tau^{-1} \\ &= \tau(\sigma'_1 \ldots \sigma'_m)\tau^{-1} \\ &= \tau\sigma'_1(\tau^{-1}\tau)\sigma'_2(\tau^{-1}\tau)\ldots(\tau^{-1}\tau)\sigma'_m\tau^{-1} \\ &= (\tau\sigma'_1\tau^{-1})(\tau\sigma'_2\tau^{-1})\ldots(\tau\sigma'_m\tau^{-1}).\end{aligned}$$

  By Exercise 3.4.1, we know that if σ'_i is a j-cycle, then $\tau\sigma'_i\tau^{-1}$ is also a j-cycle. Then for each $\{\sigma'_i\}$, we have $\{\tau\sigma'_i\tau^{-1}\} = \{\sigma'_i\}$. Hence,

  $$\{\sigma_1\} = \sum_{i=1}^{m}\{\sigma'_i\} = \sum_{i=1}^{m}\{\tau\sigma'_i\tau^{-1}\} = \{\sigma_2\}.$$

  Then σ_1 and σ_2 have the same cycle structure.

We conclude if σ' is any other j–cycle, then σ and σ' are conjugate.

Exercise 3.4.3 Proposition 1.3.9 shows that every permutation is a composition of 2-cycles, and thus the set of all 2-cycles generates S_n (i.e. the subgroup $G < S_n$ generated by the set of all 2-cycles is all of S_n). Prove that $(1\ 2)$ and $(1\ 2\ 3\ \ldots\ n)$ generates S_n; that is, prove

$$H = \langle(1\ 2), (1\ 2\ 3\ \ldots\ n)\rangle = S_n.$$

Exercise 3.4.8 Let $n \geq 3$. Prove that $R_n = \{I, r, r^2, r^3, \ldots, r^{n-1}\} \subset D_n$, the cyclic subgroup generated by r, is a normal subgroup. This is called **the subgroup of rotations**.

We have $|D_n| = 2n$ and $|R_n| = n$. Since R_n is a cyclic subgroup of D_n, by (Lagrange's Theorem),

$$[D_n : R_n] = |D_n|/|R_n| = 2.$$

By Exercise 3.5.4, R_n is a normal subgroup.

Exercise 3.5.1 Prove *Fermat's Little Theorem:* For every prime $p \geq 2$ and $a \in \mathbb{Z}$, we have $a^p \equiv a \mod p$.

Exercise 3.5.4 Suppose G is a group and $N < G$ is a subgroup with $[G : N] = 2$. Prove that $N \triangleleft G$ is a normal subgroup.

By Lagrange's Theorem, $|G/N| = [G : N] = 2$. Then the number of left cosets is 2. Note that every element $g \in G$ is in some coset. Hence, $g \in G$ implies $g \in g_1N \cup g_2N$ for some $g_1 \in N$ and $g_2 \in G - N$. Then $G \subset g_1N \cup g_2N$. For $g \in g_1N \cup g_2N$, since $N \subset G$, $g_1, g_2 \in G$, $g_1N \cup g_2N \subset G$. Hence, $G = g_1N \cup g_2N$. Since $g_1 \in N$, $g_1N = N$. Then $G = N \cup gN$ for some $g \in G - N$. Note that $G = N \cup G - N$. Then $gN = G - N$ for some $g \in G - N$. Similarly, $Ng = G - N$ for some $g \in G - N$.

- $g \in N$: $gN = N = Ng$.
- $g \in G - N$: We have $gN = G - N$ and $Ng = G - N$. Then $gN = Ng$.

We conclude for all $g \in G$, $gN = Ng$. Hence, $N \triangleleft G$ is a normal subgroup.