Solution for Homework 8

Xiangcan Li

March 24, 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

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

By Exercise 3.4.1, we have $\tau\sigma\tau^{-1} = (\tau(k_1)\ \tau(k_2)\ \ldots\ \tau(k_j))$, where $\sigma = (k_1\ k_2\ \ldots\ k_j)$.
Then we have

$$\begin{aligned}\tau\sigma\tau^{-1} &= (1\ \ldots\ n)(1\ 2)(1\ \ldots\ n)^{-1} = (\tau(1)\ \tau(2)) = (2\ 3) \\ \tau\sigma\tau^{-1} &= (1\ \ldots\ n)(2\ 3)(1\ \ldots\ n)^{-1} = (\tau(1)\ \tau(2)) = (3\ 4) \\ &\vdots \\ \tau\sigma\tau^{-1} &= (1\ \ldots\ n)(n-2\ n-1)(1\ \ldots\ n)^{-1} = (\tau(1)\ \tau(2)) = (n-1\ n).\end{aligned}$$

We also have

$$(1\ 2)(2\ 3)(1\ 2) = (1\ 3)$$
$$\vdots$$
$$(1\ n-1)(n-1\ n)(1\ n-1) = (1\ n).$$

For $(i,j) \in S_n$, where $i \neq j, i, j \in [1,n]$ and $i, j \in \mathbb{Z}$, we have

$$\tau\sigma\tau^{-1} = (1\ i)(1\ j)(1\ i)^{-1} = (\tau(1)\ \tau(j)) = (i\ j).$$

Note that all 2-cycle can be in the form of $(i\ j)$. Any (i,j) can be represent in the form of $(1\ i)(1\ j)(1\ i)^{-1}$, where $(1\ i)$ and $(1\ j)$ can be written as a composition of three cycles $(1\ i-1)(i-1\ i)(1\ i-1)$ and $(1\ j-1)(j-1\ j)(1\ j-1)$, respectively. We have shown above that $(1\ i-1), (i-1\ i), (1\ j-1), (j-1\ j)$ can be written as composition of $(1\ 2)$ and $(1\ \dots\ n)$. Then all the 2-cycle can be written as composition of $(1\ 2)$ and $(1\ \dots\ n)$. Since the set of all 2-cycle generates S_n, and $(1\ 2), (1\ \dots\ n)$ generate all the 2-cycle, $(1\ 2), (1\ \dots\ n)$ generate S_n.

We conclude $H = \langle (1\ 2), (1\ 2\ 3\ \dots\ n) \rangle = S_n$..

Exercise 3.4.6 Prove $D_3 \cong S_3$.

By Exercise 3.4.3, $(1\ 2)$ and $(1\ 2\ 3)$ generates S_3. Then all elements in S_3 can be in the form of $(1\ 2\ 3)^i(1\ 2)^j$. Then we have

$$\begin{aligned}
e &= (1\ 2\ 3)^0(1\ 2)^0 \\
(1\ 2) &= (1\ 2\ 3)^0(1\ 2)^1 \\
(1\ 3) &= (1\ 2\ 3)^1(1\ 2)^1 \\
(2\ 3) &= (1\ 2\ 3)^2(1\ 2)^1 \\
(1\ 2\ 3) &= (1\ 2\ 3)^1(1\ 2)^0 \\
(1\ 3\ 2) &= (1\ 2\ 3)^2(1\ 2)^0
\end{aligned}$$

Consider $\phi : S_3 \to D_3$ be

$$\begin{aligned}
\phi(e) &= \phi((1\ 2\ 3)^0(1\ 2)^0) = r^0 j^0 = I \\
\phi(1\ 2) &= \phi((1\ 2\ 3)^0(1\ 2)^1) = r^0 j^1 \\
\phi(1\ 3) &= \phi((1\ 2\ 3)^1(1\ 2)^1) = r^1 j^1 \\
\phi(2\ 3) &= \phi((1\ 2\ 3)^2(1\ 2)^1) = r^2 j^1 \\
\phi(1\ 2\ 3) &= \phi((1\ 2\ 3)^1(1\ 2)^0) = r^1 j^0 \\
\phi(1\ 3\ 2) &= \phi((1\ 2\ 3)^2(1\ 2)^0) = r^2 j^0.
\end{aligned}$$

We observe that $\phi((1\ 2\ 3)^i(1\ 2)^k) = r^i j^k$ for $i \in \{0,1,2\}$ and $k \in \{0,1\}$.
Note that $r^m j^n = j^{-n} r^m$ and $(1\ 2\ 3)^s(1\ 2)^t = (1\ 2)^{-t}(1\ 2\ 3)^s$.
Then for $(1\ 2\ 3)^p(1\ 2)^q, (1\ 2\ 3)^{p'}(1\ 2)^{q'} \in S_3$, we have

$$\begin{aligned}
\phi((1\ 2\ 3)^p(1\ 2)^q(1\ 2\ 3)^{p'}(1\ 2)^{q'}) &= \phi((1\ 2\ 3)^p(1\ 2\ 3)^{-p'}(1\ 2)^q(1\ 2)^{q'}) \\
&= \phi((1\ 2\ 3)^{p-p'}(1\ 2)^{q+q'}) \\
&= r^{p-p'} j^{q+q'} \\
&= r^p r^{-p'} j^q j^{q'} \\
&= r^p j^q r^{p'} j^{q'} \\
&= \phi((1\ 2\ 3)^p(1\ 2)^q)\phi((1\ 2\ 3)^{p'}(1\ 2)^{q'})
\end{aligned}$$

Note that if $p - p' < 0$, we have $r^{p-p'} j^{q+q'} = j^{q+q'} r^{p'-p}$ and will get the same result.
Then ϕ is a homomorphism. Clearly, ϕ is also bijective. Hence, ϕ is isomorphism.
We conclude $D_3 \cong S_3$.

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 $a^p \equiv a \mod p$.

- Suppose $p \mid a$, then $a = kp$ for some $k \in \mathbb{Z}$. Then $a^p - a = (kp)^p - kp = k^p p^{p-1} p - kp = (k^p p^{p-1} - k)p$, where $k^p p^{p-1} - k \in \mathbb{Z}$. Hence, $a^p \equiv a \mod p$.
- Suppose $p \nmid a$. Since p is a prime, the divisor of p is 1 and p. Since p is not a divisor of a, $\gcd(a, n) = 1$. We have $[a] \in \mathbb{Z}_p^\times$. By Corollary 1.5.7, $\mathbb{Z}_p^\times = \mathbb{Z}_p - \{0\}$. By Example 3.2.7, $|\mathbb{Z}_p|= p$. Hence, $|\mathbb{Z}_p^\times|= p - 1$. By Corollary 3.5.7, since $\mathbb{Z}_p^\times$ is a finite group, $|[a]| \Big| |\mathbb{Z}_p^\times|$. Suppose $|[a]|= n$, then $n \mid p - 1$. By Proposition 3.2.6, $[a]^n = [1]$, the identity in $\mathbb{Z}_p^\times$. Therefore, $[a^n] = [1]$.

  Then for some $k \in \mathbb{Z}$ such that $kn = p - 1$, we have $[a^p] = [a^{(p-1)+1}] = [a^{kn+1}] = [a^n]^k [a] = [1]^k [a] = [a]$. It follows that $a^p \equiv a \mod p$.

We conclude 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 $g \in g_1 N \cup g_2 N$ for some $g_1 \in N$ and $g_2 \in G - N$. Then $G \subset g_1 N \cup g_2 N$. For $g \in g_1 N \cup g_2 N$, since $N \subset G$, $g_1, g_2 \in G$, $g_1 N \cup g_2 N \subset G$. Hence, $G = g_1 N \cup g_2 N$. Since $g_1 \in N$, $g_1 N = N$. 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.

Exercise 3.5.6 Suppose $K, H < G$ are subgroups of a group G. Prove that for all $g \in G, H \cap gK$ is either empty, or is equal to a coset of $K \cap H$ in H. Using this, prove that

$$[H : K \cap H] \leq [G : K].$$

Note that $K \cap H$ is a subgroup of G and $\{e\} \subset K \cap H$.
If $H \cap gK \neq \emptyset$, then for all $x \in H \cap gK$, we have $x \in H$ and $x \in gK$, thus $x = gk$ for some $k \in K$.

- $g \in H$. Since $x \in H, g^{-1} \in H$ and $k = g^{-1}x$, we have $k \in H$. Then $k \in K \cap H$. Therefore, $x \in g(K \cap H)$, which implies $H \cap gK \subset g(K \cap H)$. On the other hand, for all $y \in g(K \cap H)$. $y \in gK$ and $y \in gH$. Note that $gH = H$. Hence, $y \in H$ and $y \in gK$, which implies $y \in H \cap gK$. Then $g(K \cap H) \subset H \cap gK$. We conclude $g(K \cap H) = H \cap gK$.
- $g \notin H$. If $k \in H$, then $k^{-1} \in H$. Since $x \in H$, $g = xk^{-1} \in H$, a contradiction. Hence, $k \notin H$.

  Let $y \in H \cap gK$. Then $y \in H$ and $y = gl$ for some $l \in K$. Since $k, l \in K \subset G$, by Lemma 3.5.3, we have $l^{-1}k \in H$. Then $x = gk = gll^{-1}k = (gl)l^{-1}k = yl^{-1}k \in yH$. Note that $l^{-1} \in K$, then $l^{-1}k \in K$. Hence, $x \in yK$. Therefore, $x \in y(K \cap H)$, which implies $H \cap gK \subset y(K \cap H)$.

  For all $z \in y(K \cap H)$, we have $z \in yK$ and $z \in yH$. Since $y \in H$, $yH = H$. Since $l \in K$, $lK = K$. Then $yK = glK = gK$. Hence, $z \in gK$, which implies $z \in H \cap gK$. Then $y(K \cap H) \subset H \cap gK$.

  We conclude $y(K \cap H) = H \cap gK$.

For both cases, $H \cap gK$ is equal to a coset of $K \cap H$ in H.

Consider $\phi : H/K \cap H \to G/K$ as $\phi(g(K \cap H)) = gK$ for all $g \in H$.

We first prove that $\phi(g(K \cap H)) = gK$ is a well-defined map from $H/K \cap H$ to G/K. That is, we suppose $g_1(K \cap H) = g_2(K \cap H)$, and prove that $g_1K = g_2K$. Since $K \cap H$ is a subgroup of G, g_1 and g_2 belong to the same left coset of $K \cap H$. By Lemma 3.5.3, $g_1^{-1}g_2 \in K \cap H$. Then $g_1^{-1}g_2 \in K$. Since K is a subgroup of G, by Lemma 3.5.3, we have $g_1K = g_2K$. Hence, ϕ is well-defined.

For all $g_1(K \cap H), g_2(K \cap H) \in H/(K \cap H)$, if $\phi(g_1(K \cap H)) = \phi(g_2(K \cap H))$, then $g_1K = g_2K$.

Note that $g_1, g_2 \in H$. Then $g_1e \in g_1K$ and $g_1e = g_1 \in H$. Hence, $H \cap g_1K \neq \emptyset$. Similarly, $H \cap g_2K \neq \emptyset$.

Then $H \cap g_1K = g_1(K \cap H)$ and $H \cap g_2K = g_2(K \cap H)$. Since $g_1K = g_2K$, $H \cap g_1K = H \cap g_2K$. Then $g_1(K \cap H) = g_2(K \cap H)$.

We conclude ϕ is injective. Hence, $|H/K \cap H| \leq |G/K|$, i.e., $[H : K \cap H] \leq [G : K]$.