HOMEWORK 3: SOLUTIONS - MATH 341
INSTRUCTOR: George Voutsadakis

Problem 1 *(a) Show that if G is a group and $a, b \in G$, then $|aba^{-1}| = |b|$.*

(b) Show that if G is a group and $a, b \in G$, then $|ab| = |ba|$.

Solution:

(a) We show that $\{n > 0 : (aba^{-1})^n = e\} = \{n > 0 : b^n = e\}$. This will immediately imply that $|aba^{-1}| = |b|$. We have

$$\begin{aligned}
(aba^{-1})^n = e &\iff \underbrace{(aba^{-1})(aba^{-1})\dots(aba^{-1})}_{n} = e \\
&\iff a\underbrace{bb\dots b}_{n}a^{-1} = e \\
&\iff ab^na^{-1} = e \\
&\iff b^n = a^{-1}ea \\
&\iff b^n = e
\end{aligned}$$

(b) Similarly, we show that $\{n > 0 : (ab)^n = e\} = \{n > 0 : (ba)^n = e\}$. We have

$$\begin{aligned}
(ab)^n = e &\iff \underbrace{(ab)(ab)\dots(ab)}_{n} = e \\
&\iff a\underbrace{(ba)(ba)\dots(ba)}_{n-1}b = e \\
&\iff ba\underbrace{(ba)(ba)\dots(ba)}_{n-1}bb^{-1} = beb^{-1} \\
&\iff \underbrace{(ba)(ba)\dots(ba)}_{n} = e \\
&\iff (ba)^n = e.
\end{aligned}$$

■

Problem 2 *(a) List all the cyclic subgroups of S_3. Does S_3 have a noncyclic proper subgroup?*

(b) List all the cyclic subgroups of D_4. Does D_4 have a noncyclic proper subgroup?

Solution:

(a) Recall that $S_3 = \{1, (12), (13), (23), (123), (132)\}$. Checking one by one all the subgroups generated by a single element we get the following cyclic subgroups:

$$\begin{aligned}
&1 = \langle e\rangle \\
&\{1, (12)\} = \langle (12)\rangle \\
&\{1, (13)\} = \langle (13)\rangle \\
&\{1, (23)\} = \langle (23)\rangle \\
&\{1, (123), (132)\} = \langle (123)\rangle = \langle (132)\rangle.
\end{aligned}$$

It is not very tough to see that adjoining to any cyclic subgroup of order 2 an element of order 3 or to any cyclic subgroup of order 3 an element of order 2 will yield the whole group S_3. Thus, there are no noncyclic proper subgroups of S_3.

(b) Recall that $D_4 = \{\rho_0, \rho, \rho^2, \rho^3, \tau, \rho\tau, \rho^2\tau, \rho^3\tau\}$. Again we may check that the list of its cyclic subgroups is

$$\begin{aligned}
&1 = \langle \rho_0 \rangle \\
&\{\rho_0, \rho, \rho^2, \rho^3\} = \langle \rho \rangle = \langle \rho^3 \rangle \\
&\{\rho_0, \rho^2\} = \langle \rho^2 \rangle \\
&\{\rho_0, \tau\} = \langle \tau \rangle \\
&\{\rho_0, \rho\tau\} = \langle \rho\tau \rangle \\
&\{\rho_0, \rho^2\tau\} = \langle \rho^2\tau \rangle \\
&\{\rho_0, \rho^3\tau\} = \langle \rho^3\tau \rangle
\end{aligned}$$

$G = \{\rho_0, \rho^2, \tau, \rho^2\tau\}$ is a noncyclic proper subgroup of D_4.

■

Problem 3 *Let G be a group with no nontrivial proper subgroups.*

(a) Show that G must be cyclic.

(b) What can you say about the order of G?

Solution:

(a) If $G = \{e\}$, then $G = \langle e \rangle$, whence G is cyclic. On the other hand, if $G \neq \{e\}$, there must be an $a \in G, a \neq e$. Consider the cyclic subgroup $\langle a \rangle$ generated by a. We have $\{e\} \neq \langle a \rangle \leq G$. Hence, since G does not have any nontrivial proper subgroups, we must have $\langle a \rangle = G$ and, therefore, G is cyclic with generator a.

(b) In part (a) we showed that any nonidentity element of the group must be a generator of the group. Thus, the order n of the generator a must be such that all $a^k, 0 < k < n$, are generators of G. This is the case if and only if n is a prime.

■

Problem 4 *Let* $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 4 & 1 & 6 & 7 & 2 & 5 \end{pmatrix}$ *and* $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 1 & 2 & 7 & 8 & 5 & 3 \end{pmatrix}$. *Calculate:*

(a) $\phi\tau$ and $\tau\phi$

(b) $\phi^2\tau$ and $\phi\tau^2$

(c) the inverses ϕ^{-1} and τ^{-1}

(d) the orders $|\phi|$ and $|\tau|$.

Solution:

(a)

$$\begin{aligned} \phi\tau &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 4 & 1 & 6 & 7 & 2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 1 & 2 & 7 & 8 & 5 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 1 & 3 & 8 & 2 & 5 & 6 & 4 \end{pmatrix}. \\ \tau\phi &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 1 & 2 & 7 & 8 & 5 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 4 & 1 & 6 & 7 & 2 & 5 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 2 & 6 & 8 & 5 & 4 & 7 \end{pmatrix} \end{aligned}$$

(b)

$$\begin{aligned} \phi^2\tau &= \phi(\phi\tau) \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 4 & 1 & 6 & 7 & 2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 1 & 3 & 8 & 2 & 5 & 6 & 4 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 8 & 6 & 7 & 1 \end{pmatrix}. \\ \phi\tau^2 &= (\phi\tau)\tau \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 1 & 3 & 8 & 2 & 5 & 6 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 1 & 2 & 7 & 8 & 5 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 8 & 7 & 1 & 6 & 4 & 2 & 3 \end{pmatrix} \end{aligned}$$

(c)

$$\begin{aligned} \phi^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 4 & 1 & 6 & 7 & 2 & 5 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 1 & 3 & 8 & 5 & 6 & 2 \end{pmatrix}. \\ \tau^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 1 & 2 & 7 & 8 & 5 & 3 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 8 & 2 & 7 & 1 & 5 & 6 \end{pmatrix} \end{aligned}$$

(d)

$$\begin{aligned} \phi &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 4 & 1 & 6 & 7 & 2 & 5 \end{pmatrix} \\ &= (134)(28567). \\ \tau &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 1 & 2 & 7 & 8 & 5 & 3 \end{pmatrix} \\ &= (1386)(24)(57). \end{aligned}$$

From the above cyclic decompositions we can easily see that $|\phi| = 15$ and $|\tau| = 4$.

■

Problem 5 *(a) Show that if ρ and σ in S_n are disjoint cycles, and $\phi = \rho\sigma$, then $|\phi| = \mathrm{lcm}(|\rho|, |\sigma|)$.*

(b) Show that an m-cycle is an even permutation if and only if m is odd.

Solution:

(a) We need to show that $\phi^{\mathrm{lcm}(|\rho|,|\sigma|)} = 1$ and that, for no $0 < n < \mathrm{lcm}(|\rho|, |\sigma|)$ is it the case that $\phi^n = 1$. Let $l = \mathrm{lcm}(|\rho|, |\sigma|)$. Then $l = p|\rho| = q|\sigma|$, for some integers p, q. Thus

$$\begin{aligned} \phi^l &= (\rho\sigma)^l \\ &= \rho^l \sigma^l \\ &= \rho^{p|\rho|}\sigma^{q|\sigma|} \\ &= 1 \cdot 1 \\ &= 1. \end{aligned}$$

Now, if $\phi^n = 1$, we must have $(\rho\sigma)^n = 1$, whence $\rho^n\sigma^n = 1$. Since ρ and σ are disjoint, this yields $\rho^n = 1$ and $\sigma^n = 1$. For this to happen $|\rho|\backslash n$ and $|\sigma|\backslash n$, whence $l\backslash n$, i.e., $l \leq n$.

(b) Let $\phi = (a_1 a_2 \dots a_m)$ be an m-cycle. Then $\phi = (a_1 a_{m-1})(a_1 a_{m-2}) \dots (a_1 a_2)$. Thus ϕ is even if and only if $m - 1$ is even, i.e., if and only if m is odd.

■