1. Let G be a group, $a \in G$ and $f : G \to G$ is defined by $x \mapsto ax$. Determine if f is injective, and if it is surjective. Provide proof or counterexample of your claims.

   Proof. Let $x, y \in G$. Hence $f(x) = ax$ and $f(y) = ay$. Then, Let $f(x) = f(y)$ and we need to proof it implies $x = y$ for it to be injective.

$$\begin{aligned} f(x) &= f(y) \\ ax &= ay \\ a^{-1}ax &= a^{-1}ay \\ x &= y \end{aligned}$$

   Hence, f is injective.
   Let $y \in G$, such that for all element y, there exist $x \in G$ such that $f(x) = y$.

$$\begin{aligned} y &= ax \\ a^{-1}y &= a^{-1}ax \\ x &= a^{-1}y \end{aligned}$$

   Since both a^{-1} and y are in G, x must also be in G. Therefore, for all $y \in G$, there exist $f(a^{-1}y) = aa^{-1}y = y$, which indicates that f is also surjective.

   ■

2. Let $f : A \to B$ and $g : B \to A$. Suppose that $f(x) = y$ iff $g(y) = x$. Prove that f is bijective (and that $g = f^{-1}$).

   Proof. We need to prove f is bijective that is f is both injective and surjective.
   First, suppose that $f(x_1) = f(x_2)$ for some x_1, x_2 in A. We need to show that $x_1 = x_2$. Since $f(x_1) = f(x_2)$, we have $g(f(x_1)) = g(f(x_2))$. By the statement, it implies that $x_1 = x_2$. Therefore, f is injective.

   Then, let $y \in B$, and we need to show that there exists an x in A such that $f(x) = y$. Since, g is from B to A, there is x such that $g(y) = x$. Then, by the condition, we will have $f(x) = y$. Therefore, f is surjective and hence bijective.

   We know that $f(x) = f(g(y)) = y$ and $g(f(x)) = g(y) = x$. If $x = y$, then $f(g(y)) = g(f(x)) = y = x$, which implies that $g = f^{-1}$. ■

3. Let $A = \{x \in \mathbb{R} \mid x \neq 0, 1\}$ and $G = \{\epsilon, f, g, h, j, d\}$, where

$$\epsilon = x \qquad f = 1 - x \qquad g = \frac{1}{x}$$
$$h = \frac{1}{1-x} \qquad j = \frac{x-1}{x} \qquad d = \frac{x}{x-1}$$

Show that $G \leq S_A$, and write the table out for G. (HINT: let the table do the heavy lifting for you.)

Proof. To show that $G \leq S_A$, we need to show that G is a subgroup of S_A. Since $x \in \mathbb{R}$ and $x \neq 0, 1$, all element in G is in real number, hence in A. S_A contains all permutations of A. Therefore, G must be a nonempty subset of S_A.

Then, we need to show that G is closed under function composition operation. We can prove it by building the table.

$\epsilon \cdot \epsilon = \epsilon \cdot x = x = \epsilon$
$\epsilon \cdot f = \epsilon \cdot (1 - x) = 1 - x = f$
$\epsilon \cdot g = \epsilon \cdot \frac{1}{x} = \frac{1}{x} = g$
$\epsilon \cdot h = \epsilon \cdot \frac{1}{1-x} = \frac{1}{1-x} = h$
$\epsilon \cdot j = \epsilon \cdot \frac{x-1}{x} = \frac{x-1}{x} = j$
$\epsilon \cdot d = \epsilon \cdot \frac{x}{x-1} = \frac{x}{x-1} = d$

$f \cdot \epsilon = f(x) = 1 - x = f$
$f \cdot f = f(f(x)) = f(1 - x) = x = \epsilon$
$f \cdot g = f(g(x)) = f(\frac{1}{x}) = 1 - \frac{1}{x} = \frac{x-1}{x} = j$
$f \cdot h = f(h(x)) = f(\frac{1}{1-x}) = \frac{x}{1-x} = d$
$f \cdot j = f(j(x)) = f(\frac{x-1}{x}) = \frac{1}{x} = g$
$f \cdot d = f(d(x)) = f(\frac{x}{x-1}) = \frac{x-1-x}{x-1} = -\frac{1}{x-1} = \frac{1}{1-x} = h$

$g \cdot \epsilon = g(x) = \frac{1}{x} = g$
$g \cdot f = g(f(x)) = g(1 - x) = \frac{1}{1-x} = h$
$g \cdot g = g(g(x)) = g(\frac{1}{x}) = x = \epsilon$
$g \cdot h = g(h(x)) = g(\frac{1}{1-x}) = 1 - x = f$
$g \cdot j = g(j(x)) = g(\frac{x-1}{x}) = \frac{x}{x-1} = d$
$g \cdot d = g(d(x)) = g(\frac{x}{x-1}) = \frac{1}{\frac{x}{x-1}} = \frac{x-1}{x} = j$

$h \cdot \epsilon = h(x) = \frac{1}{1-x} = h$
$h \cdot f = h(f(x)) = h(1 - x) = \frac{1}{1-(1-x)} = \frac{1}{x} = g$
$h \cdot g = h(g(x)) = h(\frac{1}{x}) = \frac{1}{1-\frac{1}{x}} = \frac{1}{\frac{x-1}{x}} = \frac{x}{x-1} = d$

$h \cdot h = h(h(x)) = h(\frac{1}{1-x}) = \frac{1}{1-\frac{1}{1-x}} = \frac{1}{\frac{x}{x-1}} = \frac{x-1}{x} = j$
$h \cdot j = h(j(x)) = h(\frac{x-1}{x}) = \frac{1}{1-\frac{x-1}{x}} = \frac{1}{\frac{1}{x}} = x = \epsilon$
$h \cdot d = h(d(x)) = h(\frac{x}{x-1}) = \frac{1}{1-\frac{x}{x-1}} = \frac{1}{\frac{1}{1-x}} = f$

$j \cdot \epsilon = j(x) = \frac{x-1}{x} = j$
$j \cdot f = j(f(x)) = j(1-x) = \frac{1-x-1}{1-x} = \frac{x}{x-1} = d$
$j \cdot g = j(g(x)) = j(\frac{1}{x}) = \frac{\frac{1}{x}-1}{\frac{1}{x}} = 1 - x = f$
$j \cdot h = j(h(x)) = j(\frac{1}{1-x}) = \frac{\frac{1}{1-x}-1}{\frac{1}{1-x}} = \frac{\frac{x}{1-x}}{\frac{1}{1-x}} = x = \epsilon$
$j \cdot j = j(j(x)) = j(\frac{x-1}{x}) = \frac{\frac{x-1}{x}-1}{\frac{x-1}{x}} = \frac{1}{1-x} = h$
$j \cdot d = j(d(x)) = j(\frac{x}{x-1}) = \frac{\frac{1}{x-1}}{\frac{x}{x-1}} = \frac{1}{x} = g$

$d \cdot \epsilon = d(x) = \frac{x}{x-1} = d$
$d \cdot f = d(f(x)) = d(1-x) = \frac{1-x}{1-x-1} = \frac{1-x}{-x} = \frac{x-1}{x} = j$
$d \cdot g = d(g(x)) = d(\frac{1}{x}) = \frac{\frac{1}{x}}{\frac{1}{x}-1} = \frac{1}{1-x} = h$
$d \cdot h = d(h(x)) = d(\frac{1}{1-x}) = \frac{\frac{1}{1-x}}{\frac{1}{1-x}-1} = \frac{1}{x} = g$
$d \cdot j = d(j(x)) = d(\frac{x-1}{x}) = \frac{\frac{x-1}{x}}{\frac{x-1}{x}-1} = \frac{x-1}{-1} = 1 - x = f$
$d \cdot d = d(d(x)) = d(\frac{x}{x-1}) = \frac{\frac{x}{x-1}}{\frac{x}{x-1}-1} = \frac{x}{1} = x = \epsilon$

$\epsilon \cdot \epsilon = \epsilon$
$\epsilon \cdot f = f(\epsilon) = 1 - \epsilon = 1 - x = f$
$\epsilon \cdot g = g(\epsilon) = \frac{1}{\epsilon} = \frac{1}{x} = g$
$\epsilon \cdot h = h(\epsilon) = \frac{1}{1-\epsilon} = \frac{1}{1-x} = h$
$\epsilon \cdot j = j(\epsilon) = \frac{\epsilon-1}{\epsilon} = \frac{x-1}{x} = j$
$\epsilon \cdot d = d(\epsilon) = \frac{\epsilon}{\epsilon-1} = \frac{x}{x-1} = d$

$\circ$	ϵ	f	g	h	j	d
ϵ	ϵ	f	g	h	j	d
f	f	ϵ	j	d	g	h
g	g	h	ϵ	f	d	j
h	h	g	d	j	ϵ	f
j	j	d	f	ϵ	h	g
d	d	j	h	g	f	ϵ

By exhaustion, we proved that the group is closed under the composite function(for all operations the result is unique and within the group). Also, noticing that the inverse is all defined because all elements can composite with one other element such that their product is the identity. Therefore, G is a subgroup of S_A. ■

4. Let α and β be disjoint cycles:

$$\alpha = (a_1\ a_2 ... a_s) \qquad \beta = (b_1\ b_2 ... b_r)$$

(a) Prove that for $n \in \mathbb{Z}^+$, $(\alpha\beta)^n = \alpha^n\beta^n$.

Proof. Since α and β are disjoint hence commute. That is $\alpha\beta = \beta\alpha$.

$$\begin{aligned}\alpha^n\beta^n &= \alpha ... \alpha\alpha\alpha\beta\beta\beta ... \beta \\ &= \alpha ... \alpha\alpha\beta\alpha\beta\beta ... \beta \\ &= \alpha ... \alpha\beta\alpha\beta\alpha\beta ... \beta\end{aligned}$$

keep substituting $\alpha\beta$ with $\beta\alpha$ until the first two cycles are $\alpha\beta$ we will have:

$$= \alpha\beta ... \alpha\beta$$

Noticing that the total number of cycle α and β is fixed, $\alpha\beta$ will repeat n times, hence $\alpha^n\beta^n = (\alpha\beta)^n$.

■

(b) Find a transposition γ such that $\alpha\beta\gamma$ is a cycle. Then show that $\alpha\gamma\beta$ and $\gamma\alpha\beta$ are cycles.

Solution. Since α and β are disjoint, γ must carry some b to some a. We can make it to carry the last element of b to the first element of a. That is $\gamma = (a_1, b_r)$. We will have $(a_1\ a_2 ... a_s)(b_1\ b_2 ... b_r)(a_1, b_r)$. a_1 will be carried to b_r and then to b_1. Then, b_1 will be carried to b_2,b_2 to b_3 until b_{r-1} to b_r. b_r will be carried to a_1 and then a_2. Lastly, a_2 will be carried to a_3, a_3 to a_4 until a_{s-1} to a_s. Lastly, a_s will be carried to a_1 which goes back to b_1. Therfore, when $\gamma = (a_1, b_r)$, $\alpha\beta\gamma = (a_1\ a_2 ... a_s)(b_1\ b_2 ... b_r)(a_1, b_r) = (a_1 b_1 b_2 ... b_r a_2 a_3 ... a_s)$, which is a cycle.

For $\alpha\gamma\beta$, we have $(a_1\ a_2 ... a_s)(a_1, b_r)(b_1\ b_2 ... b_r)$. Starting with b_1, it will be carried to b_2, b_2 to b_3 ... until b_{r-2} is carried to b_{r-1}. Then, b_{r-1} will be carried to b_r in the third cycle, to a_1 in the second cycle and to a_2 in the first cycle. Continuing with a_2, it will be carried to a_3, a_3 to a_4 ... until a_{s-1} is carried to a_s. Then, a_s will be carried to a_1. Lastly, a_1 will be carried to b_r. The cycle will then be $(b_1 b_2 ... b_{r-1} a_2 a_3 ... a_s a_1 b_r)$

For $\gamma\alpha\beta$, we have $(a_1, b_r)(a_1\ a_2 ... a_s)(b_1\ b_2 ... b_r)$. Startinig with b_1, it will be carried to b_2 and then b_2 to b_3... until b_{r-1} to b_r and then to a_1. Then a_1 will be carried to a_2, a_2 to a_3...until a_{s-1} to a_s. a_s will be carried to a_1 and then b_r. Lastly, b_r will be carried back to b_1, finishes the permutation. Therefore, we can conclude that $\gamma\alpha\beta = (a_1, b_r)(a_1\ a_2 ... a_s)(b_1\ b_2 ... b_r) = (b_1 b_2 ... b_{r-1} a_1 a_2 ... a_s b_r)$, which is a cycle. □

5. If π is a permutation in S_n, and α is a cycle, we call $\pi\alpha\pi^{-1}$ a **conjugate** of α. Let $\alpha = (a_1\ a_2 ... a_s)$ show that its conjugate $\pi\alpha\pi^{-1}$ is the cycle

$$(\pi(a_1)\ \pi(a_2) ... \pi(a_s)).$$

Proof. We need to show that applying $\pi\alpha\pi^{-1}$ to $\pi(a_1)$, it will be carried to $\pi(a_2)$, applying it to $\pi(a_2)$, it will be carried to $\pi(a_3)$, and so on, until applying it to $\pi(a_s)$, it can be carried to $\pi(a_1)$. Since π is a permutation in S_n, $\pi\pi_{-1} = \epsilon$.

To begin, let $i \in 1, 2, ..., s$. Then we have:

$$\begin{aligned}(\pi\alpha\pi^{-1})(\pi(a_i)) &= (\pi\alpha\pi^{-1}\pi(a_i)) \\ &= (\pi\alpha\epsilon(a_i)) \\ &= \pi\alpha(a_i)\end{aligned}$$

Since $\alpha(a_i) = a_{i+1}$ if $i \neq s$ and $\alpha(a_i) = a_1$ if $i = s$. That is $(\pi\alpha\pi^{-1})(\pi(a_i)) = \pi(a_{i+1})$ when $i \neq s$ and $(\pi\alpha\pi^{-1})(\pi(a_i)) = \pi(a_1)$ when $i = s$, which makes it equivalent to $(\pi(a_1)\ \pi(a_2) ... \pi(a_s))$. ■