Let A be a nonempty set, and let

$$S_A = \{f : A \longrightarrow A : \text{f is both 1 to 1 and onto}\}$$

Show that S_A is a group under composition. Is S_A an Abelian group?

a. **Closure:** Want to show that, ∀ f, g ∈ S_A, f o g ∈ S_A

Let f, g ∈ S_A, and let a ∈ A.

Since both f and g are well defined, f(a) and g(a) exist.

Since both f and g map to A, f(a) ∈ A and g(a) ∈ A. **(1)**

Since both f and g are one to one, f(a) and g(a) are unique. **(2)**

By **(1)** and **(2)**, f(g(a)) and g(f(a)) both exist and are unique.

Therefore, both f o g and g o f are one-to-one.

Now, we want to show that they're onto.

Suppose ∃ a_0 ∈ A such that f(g(a)) ≠ a_0 (or that g(f(a)) ≠ a_0), ∀ a ∈ A.

However, if a_0 ∈ A, then it gets mapped onto by both f and g.

So that means there exists some a_f and a_g in A such that f(a_g) = a_0 (or g(a_f) = a_0).

And since a_f and a_g are in A, they get mapped to by f and g, respectively.

Thus, a contradiction.

b. **Associativity:** Want to show that, ∀ f, g, h ∈ S_A, (f o g) o h = f o (g o h).

Let f, g, h ∈ S_A, and let a ∈ A.

Let h(a) = a_h, g(h(a)) = a_{gh}, f(a) = a_f, f(g(a)) = a_{fg}, which are all defined since f, g, and h are all well defined and onto.

Notice that ((f o g) o h)(a) = f(g(a_h)) and (f o (g o h))(a) = f(a_{gh}).

Want to show: g(a_h) = a_{gh}.

Well, g(a_h) = g(a(h)) by definition, and a_{gh} = g(a(h)) by definition.

Hence, result.

c. **Identity:** Want to show that ∃ I ∈ S_A such that I o f = f o I = f, ∀ f ∈ S_A.

Define I : A ⟶ A to be I(a) = a, ∀ a ∈ A.

Want to show: I is well defined.

Let a ∈ A.

Then I(a) = a. Since all elements of A are unique, all I(a)'s are unique.

Hence, I is well defined.

Want to show: I is one-to-one.

Let I(a_1) = I(a_2).

Since I(a) = a, a_1 = a_2.

Want to show: I is onto.

Let a ∈ A, the set that I maps into.

Since I(a) = a, a is the element that maps to a.

Want to show: I $\in$ $\mathbf{S}_A$

Since I is one-to-one and onto, I $\in$ S_A.

Want to show: I o f = f o I = f.

Let f $\in$ S_A and a $\in$ A.

Notice that f(I(a)) = f(a) and I(f(a)) = f(a).

Hence, result.

d. **Inverse:** Want to show that, $\forall$ f $\in$ S_A, $\exists$ f^{-1} such that $f(f^{-1}(a)) = f^{-1}(f(a)) = a$, $\forall$ a $\in$ A.

Want to show: $\mathbf{f^{-1}}$ is well defined.

Let f $\in$ S_A and suppose we have a relation f^{-1} such that $f^{-1}(f(a)) = a$.

We know that f is one-to-one. Thus, if $f(a_1) = f(a_2)$, then $a_1 = a_2$.

Therefore there is no f(a) such that $f^{-1}(f(a))$ has two outputs.

Hence, f^{-1} is a well-defined function.

Want to show: $\mathbf{f^{-1}}$ is one-to-one.

Suppose $\exists$ a $\in$ A such that $f^{-1}(f(a_1)) = a$ and $f^{-1}(f(a_2)) = a$ for some $a_1, a_2 \in A$ $(a_1 \neq a_2)$

We know that, since f is one-to-one, $f(a_1) \neq f(a_2)$.

So, by definition of f^{-1}, f^{-1} has to map $f(a_1)$ and $f(a_2)$ back to a_1 and a_2, respectively.

A contradiction.

Want to show: $\mathbf{f^{-1}}$ is onto.

Suppose $\exists$ $a_0 \in A$ such that $f^{-1}(f(a)) \neq a_0$, $\forall$ a $\in$ A.

Since f is one-to-one and onto, $f(a_0)$ maps to some unique $a_f \in A$ (i.e. $f(a_0) = a_f$).

$f^{-1}(a_f)$ can only map to one solution since f^{-1} is one-to-one, which is guaranteed to exist.

Since $f^{-1}(f(a_0)) = f^{-1}(a_f)$, $f^{-1}(a_f)$ is, by definition, a_0.

A contradiction.

Want to show: $\mathbf{f^{-1} \in S_A}$

Since f^{-1} is one-to-one and onto, $f^{-1} \in S_A$.

S_A is **NOT** an Abelian group (since function composition is not commutative).