QUESTION

(a) State the three axioms A1-A3 for a group $(G, e, *)$.

(b) Show that every finite group is isomorphic to a group of permutations of a finite set.

(c) **(i)** Carefully prove the following statement using only the axioms for a group, and saying which axiom you use at each stage of the argument: Given a group $(G, e, *)$ and elements $g, h, k \in G$, if $g * h = g * k$ then $h = k$.

(ii) Use your result from the previous part to prove the following statement: Given a group $(g, e, *)$ and an element $g \in G$ there is a unique element $k \in G$ such that $g * k = e$.

(iii) Given a group $(G, e, *)$ and elements $g, k \in G$ show that if $g*k = e$ than $k * g = e$.

(d) Let $(G, e, *)$ be a group. Show that the binary operation $\cdot$ on G, defined by $a \cdot b = b * a$, is a group operation on G. Show also that the map $\phi : G \longleftarrow G$ defined by $g \mapsto g^{-1}$ is an isomorphism from the group $(G, e, *)$ to the group $(G, e, \cdot)$.

ANSWER

(a) **A1)** For any three element $g, h, k \in G, (g * h) * k = g * (h * k)$.

A2) There is an element $e \in G$ such that for any element $g \in G$, we have $e * g = g = g * e$.

A3) For any element $g \in G$ there is an element g^{-1} (called the inverse of g) such that $g * g^{-1} = g^{-1} * g = e$.

(b) For each element $g \in G$ define a function $f_g : G \Longrightarrow G$ by $f_g(k) = g * k$. This is a bijection since its inverse is given by the function $f_{g^{-1}}$. The function $\phi : G \Longrightarrow S_G$ given by $g \mapsto f_g$ is then an isomorphism since $\phi(g * h)$ is the function f_{g*h} defined by $k \mapsto (g * h) * k$, which by associativity is the same as $f_g \circ f_h(k)$, hence $\phi(g * h) = \phi(g * h) = \phi(g) \circ \phi(h)$ as required.

(c) **(i)** $g * h = g * k \Rightarrow g^{-1} * (g * h) = g^{-1} * (g * h) \Rightarrow_{A1} (g^{-1} * g) * h = (g^{-1} * g) * k \Rightarrow_{A1} e * h = e * k \Rightarrow_{A2} h = k$.

(ii) By A3 there is at least one element, denoted g^{-1} such that $g*g^{-1} = e$. Now suppose there is another denoted k. Then $g*g^{-1} = g*k \Rightarrow g^{-1} = k$ by the previous result.

(iii) $g * k = e \Rightarrow k * (g * k) = k * e =_{A2} k \Rightarrow_{A1} (k * g) * k = k \Rightarrow ((k * g) * k) * k^{-1} = k * k^{-1} =_{A3} e$. Now by A1 $((k * g) * k) * k^{-1} = (k * g) * (k * k^{-1}) =_{A3} (K * g) * e =_{A2} k * g$.

Hence $k * g = e$ as required.

(d) A1) For any elements $a, b, c \in G, a.(b.c) = (b.c) * a = (c * b) * a = c * (b * a) = (b * a).c = (a.b).c$.

A2) For any $a \in G,\ a.e = e * a = a = a * e = e.a$.

A3) For any $a \in G$ let a^{-1} denote the inverse of a for the binary operation $*$. Then $a.a^{-1} = a^{-1} * a = e = a * a^{-1} = a^{-1}.a$.

For any $a, b \in G. \phi(a * b) = (a * b)^{-1} = b^{-1} * a^{-1} = \phi(b) * \phi(a) = \phi(a), \phi(b)$, so ϕ is a homomorphism. Sine $\phi \circ \phi(a) = a$ for any $a \in G,\ \phi$ is invertible and therefore an isomorphism.