QUESTION

(a) Define the following terms:

(i) Subgroup.

(ii) Right coset.

(iii) The order of a group.

(b) State Lagrange's Theorem. Let G be a group and H a subgroup of G. Show that the relation $d \sim h \Leftrightarrow gh^{-1} \in H$ is an equivalence relation and describe its equivalence classes. Show that the equivalence classes all have the same number of elements. Use this to prove Lagrange's Theorem. Define the order of a group element and explain how and why Lagrange's Theorem constrains the order of an element in a finite group.

ANSWER

(a) **(i)** A subgroup $H < G$ is a subset $H \subseteq G$ which:

1. is closed under group multiplication $h, k \in H \Rightarrow hk \in H$
2. is closed under taking inverses:$h \in H \Rightarrow h^{-1} \in H$
3. contains the identity:$e \in H$.

(ii) The right coset $H_g = \{hg | h \in H\}$.

(iii) The order of G, $|G|$= number of elements in G.

(b) Lagrange's Theorem

If G is a finite group and H is a subgroup of G then $|H|$ divides $|G|$.

$g \sim h \Leftrightarrow gh^{-1} \in H$ is

(i) reflexive since $gg^{-1} = e \in H$

(ii) symmetric since $gk^{-1} \in H \Leftrightarrow (gk^{-1})^{-1} \in H \Leftrightarrow kg^{-1} \in H \Leftrightarrow k \sim g$

(iii) transitive since if $f \sim g \sim k$ then $fg^{-1} \in H$ and $gk^{-1} \in H$ so $f^{-1}ggk^{-1} \in H$ i.e. $fk^{-1} \in H$ and $f \sim k$

The class $[g] = \{k \in G | k \sim g\} = \{k | kg^{-1} \in H\} = \{k | k \in Hg\}$ =right coset H_g

Given two right cosets H_g and H_k define $\phi : H_g \to H_k$ by $\phi(hg) = hk$.

This is injective since $\phi(hg) = \phi(hg') \Leftrightarrow hk' \Leftrightarrow k = k'$.

It is surjective since the pre-image of hk is hg.

The equivalence classes therefore partition G into equal sized subsets, all with the same number of elements as $H = [e]$, so $|G| = n|H|$ where n is the number of distinct equivalence classes.

The order of a group element g is the least positive integer n such that $g^n = e$, or ∞ if none such exists. It is also equal to the number of elements in the cyclic subgroup $\langle g \rangle$ which must therefore divide $|G|$.