QUESTION

(a) Say what it means for a subset H of a group $(G, e, *)$ to be a subgroup.

(b) Giving brief reasons for your answer, say how many elements of S_4 lie in a subgroup generated by the two elements (12) and (234).

(c) Show that a non-empty subset H of a group $(G, e, *)$ is a subgroup if $g * h^{-1} \in H$ for all $g, h \in H$.

(d) Say what it means for a subgroup to be normal. Show that the kernel of a homomorphism is always a normal subgroup, first using the result stated in part (c) to show that it is a subgroup.

(e) State Lagrange's theorem and use it to show that any group of prime order must be cyclic.

ANSWER

(a) A subgroup of a group $(G, e, *)$ is a subset $H \subseteq G$ satisfying the following conditions.

> **S1)** If $h, k \in H$, then $h * k \in H$.
>
> **S2)** The identity element of $e \in G$ is also an element of H.
>
> **S3)** If $h \in H$ then $h^{-1} \in H$.

(b) They all do, since conjugating (12) by the powers of (234) yields the transpositions (12),(13),(14) which generate all of S_4.

(c) Since H is non empty we can choose an element $h \in H$. Putting $g = h$ we see that $e = g * h^{-1} = h * h^{-1}$ is an element of H by the hypothesis, so H satisfies axiom S2. Now given any element $h \in H$ we can put $g = e$ to get $h^{-1} = e * h^{-1}$ as an element of H, so H satisfies axiom S3. Finally given any two elements $g, h \in h$ we see that $g, h^{-1} \in H$ so $g * (h^{-1})^{-1} \in H$, or $g * h \in H$. So H also satisfies axiom S1.

(d) A subgroup $H < G$ is said to be normal if for any element $c \in G, gH = Hg$. Let $\phi : G \longleftarrow H$ be a homomorphism with kernel $K = \{g \in G | \phi(g) = e_h\}$. Clearly $e_G \in K$, so K is non-empty. Now for any $g, h \in K$ we have $\phi(gh^{-1}) = \phi(g)\phi(h)^{-1} = e_H$ so the kernel is a subgroup. Furthermore if $k \in K, g \in G$ then $\phi(g * k) = \phi(g) = \phi(k * g)$ so both gK and Kg are the pre-image of $\phi(g)$ in G hence $gK = Kg$.

(e) Lagrange's theorem: If H is a subgroup of a finite group G then $|H|$ divides $|G|$. If G has a prime order p then any subgroup of G must have order 1 or p. Take a non-trivial element $g \in G$ and consider the subgroup it generates. It has at least 2 elements, so it must have p elements, and $G = \langle g \rangle$ as required.