19-05

Práctico 8.

Ejercicio 6. Sean H y K subgrupos de un grupo G y e la unidad de G.

a. Probar que si $|H|$ y $|K|$ son coprimos entonces $H \cap K = \{e\}$.

b. Hallar los posibles valores de $|H|$ si $K \subsetneq H \subsetneq G$, $|G| = 660$ y $|K| = 66$.

a. Sea $g \in G$. Como $g \in H$, por Lagrange $o(g) \mid H$. (H y K son grupos con la operación de G)
$g \in K$, por Lagrange $o(g) \mid K$
Pero entonces $o(g) = 1$, es decir $g = e$.

b. Por Lagrange $66 \mid |H| \mid 660$
Como la inclusión es estricta, $|H| \neq 66, 660$.
Entonces $|H| = 66k$ con $k \neq 1$
$660 = |H| \cdot k' = 66kk'$ con $k, k' \neq 1$
$\Rightarrow |H| = \underset{=132}{66 \cdot 2}$ o $|H| = \underset{=330}{66 \cdot 5}$.

Ejercicio 8. Sea G un grupo. Probar las siguientes afirmaciones.

a. Si G es cíclico todo subgrupo de G también es cíclico.

b. Si G no tiene subgrupos no triviales entonces G es cíclico, finito y $|G|$ es primo.

a. Sea $H < G$.
$G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$. Queremos ver que $\exists h \in G$ tal que $H = \langle h \rangle$.

Idea: ¿g genera $\Rightarrow g * g$ genera?
Esto no es cierto en gral. Por ejemplo, en $U(7)$.
$U(7) = \{1, 2, 3, 4, 5, 6\}$
$o(1) = 2$
$\langle 2 \rangle = \{2, 4, 1\} \Rightarrow o(2) = 3$
$\langle 3 \rangle = \{3, 2, 6, 4, 5, 1\} \Rightarrow o(3) = 6$ y 3 genera $U(7)$.
Ahora, 3 genera pero $3^2 = 2$ y 2 no genera.

Otra idea: Queremos $h \in G$ que genere H. Como $h \in G$ va a ser de la forma g^k $k \in \mathbb{Z}$.

$\boxed{\text{Afirmamos que } k = \min\{n \in \mathbb{Z}^+ : g^n \in H\}. \ *}$

Veamoslo primero en el ejemplo.

Si $H = \{1, 2, 4\}$ y $g = 3$ es un generador.

$g^1 = g = 3 \notin H$

$g^2 = 2 \in H \Rightarrow k = 2$. Es decir $h = 3^2 = 2$ genera H, lo cual vimos arriba ✓.

Prueba de la afirmación $*$: sea $b \in H$. Como $b \in G \Rightarrow b = g^m$ con $m \in \mathbb{Z}$.

Dividimos entre k. $m = kq + r$, queremos ver que $r = 0$.

$$\underset{\in H}{b} = g^m = (g^k)^q \cdot g^r = \underset{\in H}{h^q} \cdot g^r.$$

$$\Rightarrow g^r = \underset{\in H}{b} \cdot \underset{\in H}{h^{-q}} \in H,$$ por minimalidad debe ser $r = 0$.

Suponemos $G \neq \{e\}$.

b. Sea $g \neq e$. $\Rightarrow \langle g \rangle = \{g, g^2, \dots\} = G$ pues es subgrupo no trivial.

Si $|G| = \infty$.

Sea $g \neq e$, como $\langle g \rangle = G$ (que es infinito) $\Rightarrow g^2 \neq e$.

De nuevo, como $\langle g^2 \rangle$ es no trivial, debe ser $\langle g^2 \rangle = G$.

Entonces $g \in \langle g^2 \rangle \Rightarrow \exists\, k$ tal que $g = g^{2k} \Rightarrow g^{2k-1} = e$ y por lo tanto $o(g) = 2k-1 \Rightarrow |G| = 2k-1 < \infty$. Esto es absurdo.

Si $|G| = nm$, existe $g \in G$ con orden nm (porque es cíclico).

Luego $g^{nm} = e \Rightarrow g^n = e$ con $g \neq e$.

$(g^n)^m = e$ y $g^n \neq e$.

En el primer caso $\langle g \rangle$ es un subgrupo no trivial y en el segundo caso $\langle g^n \rangle$ es subgrupo no trivial.