2.1. Clases laterales. Teorema de Lagrange

Relación de equivalencia determinada por un subgrupo

Sea $(G,*)$ un grupo y H un subgrupo de G. Entonces la relación definida $\forall a,b\in G$ por:
$a \sim_H b \Leftrightarrow a^{-1}*b\in H$ es relación de equivalencia en G.

La clase de equivalencia de un elemento $a\in G$ se denomina **clase lateral izquierda** módulo H y es

$$[a]_H=\{a*h : h\in H\} =^{(\text{notación})}= aH$$

Definición de índice

Sea H subgrupo del grupo $(G,*)$. Se llama **índice de** G **sobre** H al cardinal del conjunto cociente de G sobre la relación de equivalencia determinada por el subgrupo H. Dicho valor se nota por $[G:H]$.

Teorema de Lagrange

Si $(G,*)$ es un grupo finito y $H\leq G$ entonces $|H|$ es un divisor de $|G|$ y se verifica que

$$\frac{|G|}{|H|}=[G:H]$$

Corolarios

1. Si $(G,*)$ es un grupo finito de orden primo entonces G es cíclico.
2. Si $(G,*)$ es un grupo finito con $|G|=n$ entonces para todo $a\in G$ es $a^n=e$.
3. Si H y K son subgrupos de $(G,*)$ tales que $K\subset H\subset G$ entonces $[G:K]=[G:H][H:K]$

Teorema de Fermat

Si $\;p\in\mathbb{N}\;$ es primo y $\;a\not\equiv 0 \mod p\;$ entonces $\;a^{p-1}\equiv 1 \mod p$

Teorema de Euler

Si $\;\mathrm{mcd}(a,m)=1\;$ y $\;\varphi\;$ es la función de Euler, entonces $\;a^{\varphi(m)}\equiv 1 \mod m$

$$\varphi(m)=m\prod_{p\in\mathbb{N}\text{ divisor primo de } m}\left(1-\frac{1}{p}\right)$$

Teorema de Cauchy para grupos finitos

Sea $(G,*)$ un grupo de orden $n\in\mathbb{N}$.
Si $p\in\mathbb{N}$ es un divisor primo de $n\Rightarrow$ existe $a\in G$ tal que $|a|=p$

2.1.11. Problemas

1. En $(\mathbb{Z}, +)$ se considera el subgrupo $H = \{3n : n \in \mathbb{Z}\}$. Decidir cuales de los siguientes pares de clases laterales son las mismas
   a) $11 + H$ y $17 + H$
   b) $-1 + H$ y $5 + H$
   c) $7 + H$ y $23 + H$
2. Dados el grupo $(G, *)$ y $H \leq G$, calcular $|H|$ y $[G : H]$ en cada caso.
   a) $H = \langle [18]_{36} \rangle$, $(G, *) = (\mathbb{Z}_{36}, +_{36})$
   b) $H = \langle [3]_6 \rangle$, $(G, *) = (\mathbb{Z}_6, +_6)$
   c) $H = \langle [4]_{12} \rangle$, $(G, *) = (\mathbb{Z}_{12}, +_{12})$
   d) $H = \langle [12]_{60} \rangle$, $(G, *) = (\mathbb{Z}_{60}, +_{60})$
   e) $H = \langle [2]_4 \rangle \times \langle [2]_{12} \rangle$, $(G, *) = (\mathbb{Z}_4 \times \mathbb{Z}_{12}, +_4 \times +_{12})$
   f) $H = \langle ([2]_4, [2]_{12}) \rangle$, $(G, *) = (\mathbb{Z}_4 \times \mathbb{Z}_{12}, +_4 \times +_{12})$
   g) $H = \langle [1]_3 \rangle \times \langle [0]_2 \rangle \times \langle [0]_4 \rangle$, $(G, *) = (\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_4, +_3 \times +_2 \times +_4)$
   h) $H = \langle [0]_3 \rangle \times \langle [1]_2 \rangle \times \langle [2]_4 \rangle$, $(G, *) = (\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_4, +_3 \times +_2 \times +_4)$
3. Sean H y K dos subgrupos de un grupo $(G, \cdot)$ con $|G| = 660$. Si $|K| = 66$ y $K \subset H \subset G$ ¿qué orden puede tener el grupo H?
4. El grupo D_5 de las simetrías de un pentágono regular es un grupo de orden 10. Demostrar que tiene subgrupos de todos los órdenes permitidos por el teorema de Lagrange. Dar un esquema del retículo de sus subgrupos.
5. Sea $(G, *)$ un grupo y p un número primo. Demostrar que:
   a) Si G tiene orden $2p$ entonces todo subgrupo propio de G es cíclico
   b) Si G tiene orden p^2 entonces tiene un subgrupo de orden p.
6. Sean H y K dos subgrupos de un grupo $(G, *)$.
   a) Demostrar que si $|H| = 10$ y $|K| = 21$ entonces $H \cap K = \{e\}$
   b) Demostrar que si $|H| = n$ y $|K| = m$ con $\text{mcd}(n, m) = 1$ entonces $H \cap K = \{e\}$