Teorema de Lagrange

G un grupo finito

$|G|$ = cantidad de elementos de G = orden de G

H subgrupo de G

entonces $|H|$ divide a $|G|$

Ejercicio 9. Sea G un grupo con neutro e. Sean H y K subgrupos finitos de G.

a. Probar que $|H \cap K|$ divide a $\operatorname{mcd}(|H|, |K|)$.

b. Usando lo anterior, probar que si $|H|$ y $|K|$ son coprimos, entonces $H \cap K = \{e\}$.

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

a) H y K subgrupos finitos de G

queremos probar que $|H \cap K|$ divide a $\operatorname{mcd}(|H|, |K|)$

vamos a ver que $|H \cap K| \mid |H|$ y $|H \cap K| \mid |K|$

* $|H \cap K| \mid |H|$

tenemos que $H \cap K$ es subgrupo de H y H es un subgrupo finito entonces por el teorema de Lagrange $|H \cap K| \mid |H|$

* $|H \cap K| \mid |K|$

$H \cap K$ es subgrupo de K y K es un grupo finito entonces por el teorema de Lagrange $|H \cap K| \mid |K|$

H y K subgrupos de G

$H \cap K$ es un subgrupo de G

1 cerrado bajo la operación

sean $x, y \in H \cap K$, queremos ver que $x * y \in H \cap K$

$$\left.\begin{array}{l} x, y \in H \underset{H \text{ subgrupo}}{\Longrightarrow} x * y \in H \\ x, y \in K \underset{K \text{ subgrupo}}{\Longrightarrow} x * y \in K \end{array}\right\} \Rightarrow x * y \in H \cap K$$

② el neutro está en $H \cap K$

$$\left.\begin{array}{l} H \text{ subgrupo} \Rightarrow e \in H \\ K \text{ subgrupo} \Rightarrow e \in K \end{array}\right\} \Rightarrow e \in H \cap K$$

③ cerrado bajo inversos

sea $x \in H \cap K$, queremos ver que $x^{-1} \in H \cap K$

$$\left.\begin{array}{l} x \in H \underset{\substack{\uparrow \\ H \text{ subgrupo}}}{\Rightarrow} x^{-1} \in H \\ x \in K \underset{\substack{\uparrow \\ K \text{ subgrupo}}}{\Rightarrow} x^{-1} \in K \end{array}\right\} \Rightarrow x^{-1} \in H \cap K$$

$$\left.\begin{array}{l} \text{entonces } H \cap K \text{ es subgrupo de } G \\ H \text{ subgrupo de } G \\ H \cap K \subset H \end{array}\right\} \Rightarrow H \cap K \text{ subgrupo de } H$$

b) $|H|$ y $|K|$ coprimos $\Rightarrow \underbrace{H \cap K = \{e\}}_{|H \cap K| = 1}$

$|H \cap K| \mid mcd(|H|, |K|) = 1$

entonces $|H \cap K| = 1$ y por lo tanto $H \cap K = \{e\}$

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

K subgrupo de $H \underset{\substack{\uparrow \\ \text{Lagrange}}}{\Rightarrow} |K| \mid |H| \Rightarrow |H| = 66q$ para algún $q \in \mathbb{Z}$

H subgrupo de $G \underset{\substack{\uparrow \\ \text{Lagrange}}}{\Rightarrow} |H| \mid |G| \Rightarrow 66q \mid 660 \Rightarrow q \mid 10$

$66qq' = 660$

$qq' = 10$

$\Rightarrow q \mid 10$

posibilidades para q: $1, 2, 5, 10$

$q = 1$ no sirve porque $q = 1 \Rightarrow |H| = 66 \Rightarrow H = K$ ✗

$q=10$ no sirve porque $q=10 \Rightarrow H=G$ ✗

posibilidades para $|H|$ son: $66\cdot 2$, $66\cdot 5$

Ejercicio 12. Sea $f:\{1,2,\dots,n\}\to\{1,2,\dots,n\}$ una función biyectiva. Probar que el inverso de f es:

$$f^{-1} = \underbrace{f\circ f\circ\dots\circ f}_{n!-1 \text{ veces}}.$$

$$S_n = \{ f:\{1,2,\dots,n\} \to \{1,2,\dots,n\} : f \text{ biyectiva}\}$$

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & & f(n) \end{pmatrix}$$

n pos   n-1 pos   n-2 pos   1 pos

la cantidad de funciones es $n(n-1)(n-2)\cdots 1 = n!$

$|S_n| = n!$

tenemos $f\in S_n$ y queremos ver que $f^{-1} = \underbrace{f\circ f\circ\dots\circ f}_{n!-1 \text{ veces}}$

es decir queremos ver que

$$\underbrace{f\circ f\circ\dots\circ f}_{n!-1 \text{ veces}}\circ f = id$$

$$f^{n!} = \underbrace{f\circ f\circ\dots\circ f}_{n! \text{ veces}} = id$$

$$f^{|S_n|} = id$$

Vamos a probar:

$$\left.\begin{array}{l} G \text{ un grupo finito} \\ x\in G \end{array}\right\} \Rightarrow x^{|G|} = e$$

$$|\langle x\rangle| = o(x)$$

$$\langle x\rangle = \{ \overbrace{x, x^2, x^3, \dots, \underbrace{x^{o(x)}}_{e}}^{\text{son todos } \neq}, \underbrace{x^{o(x)+1}}_{x}, \underbrace{x^{o(x)+2}}_{x^2}, \dots \}$$

$\langle x\rangle$ es un subgrupo de $G \underset{\substack{\uparrow \\ \text{Lagrange}}}{\Rightarrow} |\langle x\rangle| \mid |G|$

$\Rightarrow o(x) \mid |G|$

$o(x) \mid |G| \Rightarrow |G| = o(x)\, q$ para algún $q \in \mathbb{Z}$

entonces:

$$x^{|G|} = x^{o(x) q} = \left(x^{o(x)}\right)^{q} = e^{q} = e$$

$\left.\begin{array}{l} S_n \text{ grupo finito} \\ |S_n| = n! \\ f \in S_n \end{array}\right] \Rightarrow f^{|S_n|} = id \Rightarrow \underbrace{f \circ f \circ f \cdots \circ f}_{n! \text{ veces}} = id$

$\Rightarrow \underbrace{f \circ f \cdots \circ f}_{n!-1 \text{ veces}} \circ f = id$

$\Rightarrow f^{-1} = \underbrace{f \circ f \cdots \circ f}_{n!-1 \text{ veces}}$

Ejercicio 11.

a. Probar que si $a \in U(n) \Rightarrow o(a) | \varphi(n)$.

b. i) Hallar el resto de dividir 2^{20} entre 253. Sugerencia: $2^8 = 256$.

ii) Sabiendo además que $2^{55} \equiv -45 \mod (253)$, hallar el orden de $\bar{2}$ en $U(253)$.

a) $a \in U(n) \Rightarrow o(a) \mid \varphi(n)$

$|U(n)| = \varphi(n)$

$\mathbb{Z}_n = \{\cancel{\bar{0}}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$

$U(n) = \{\bar{x} \in \mathbb{Z}_n : x \text{ es coprimo con } n\}$

$a \in U(n) \Rightarrow \langle a\rangle$ subgrupo de $U(n)$

$\underset{\substack{\uparrow \\ \text{Lagrange}}}{\Rightarrow} |\langle a\rangle| \mid |U(n)|$

$\Rightarrow o(a) \mid \varphi(n)$

$$a^{\varphi(n)} = \bar{1} \iff \underbrace{a^{\varphi(n)} \equiv 1 \pmod{n}}_{\text{teorema de Euler}}$$

Ejercicio 5. Sea G un grupo. Dado $a \in G$, probar que se cumple: $a^n = e_G \Leftrightarrow o(a)|n$.

($\Rightarrow$) $a^n = e_G$

queremos probar que $o(a)|n$

tenemos $n = o(a)q + r$ con $0 \leq r < o(a)$

queremos ver que $r = 0$

$$a^n = e_G \Rightarrow a^{o(a)q+r} = e_G$$
$$\Rightarrow a^{o(a)q} a^r = e_G$$
$$\Rightarrow (\underbrace{a^{o(a)}}_{e_G})^q a^r = e_G$$
$$\Rightarrow a^r = e_G$$

si $r \neq 0$, tendríamos $a^r = e_G$ con $1 \leq r < o(a)$ pero esto contradice la minimalidad del orden

$\Rightarrow r = 0$ y $o(a)|n$

($\Leftarrow$) $o(a)|n \Rightarrow n = o(a)q$

$$a^n = a^{o(a)q} = (\underbrace{a^{o(a)}}_{e_G})^q = e_G$$